heap_buffer_overflow_in_readScan #14

Open Cvjark opened this issue on Aug 7 · 0 comments

Cvjark commented on Aug 7 • edited

Hi, in the lastest version of this code [ps: commit id ffaf11c] I found something unusual.

crash sample

8id103_heap_buffer_overflow_in_readScan.zip

command to reproduce

```
./pdftops -q [crash sample] /dev/null
```

crash detail

```
=================================================================
==115797==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fcb48dd5800 at pc
0x00000074635f bp 0x7ffcc31156f0 sp 0x7ffcc31156e8
READ of size 4 at 0x7fcb48dd5800 thread T0
    #0 0x74635e in DCTStream::readScan() /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2549:18
    #1 0x7401e0 in DCTStream::reset() /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2257:7
    #2 0x68912e in Object::streamReset() /home/bupt/Desktop/xpdf/xpdf/./Object.h:282:13
    #3 0x68912e in Lexer::Lexer(XRef*, Object*) /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:74:12
    #4 0x581714 in Gfx::display(Object*, int) /home/bupt/Desktop/xpdf/xpdf/Gfx.cc:641:33
    #5 0x6a76a1 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, int (*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:360:10
    #6 0x6d5f6e in PSOutputDev::checkPageSlice(Page*, double, double, int, int, int, int, int,
int, int, int, int (*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PSOutputDev.cc:3276:11
    #7 0x6a7172 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, int (*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:328:13
    #8 0x6a6f81 in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*),
void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:308:3
    #9 0x6af9b4 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:384:27
    #10 0x6af9b4 in PDFDoc::displayPages(OutputDev*, int, int, double, double, int, int, int, int,
int (*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:397:5
    #11 0x796d81 in main /home/bupt/Desktop/xpdf/xpdf/pdftops.cc:342:10
    #12 0x7fcb4b949c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #13 0x41d5d9 in _start (/home/bupt/Desktop/xpdf/xpdf/pdftops+0x41d5d9)

0x7fcb48dd5800 is located 0 bytes to the right of 131072-byte region
[0x7fcb48db5800,0x7fcb48dd5800)
allocated by thread T0 here:
    #0 0x4afba0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7aa7fa in gmalloc /home/bupt/Desktop/xpdf/goo/gmem.cc:102:13
    #2 0x7aa7fa in gmallocn /home/bupt/Desktop/xpdf/goo/gmem.cc:168:10

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2549:18 in
DCTStream::readScan()
Shadow bytes around the buggy address:
  0x0ff9e91b2ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff9e91b2ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff9e91b2ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff9e91b2ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff9e91b2af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff9e91b2b00:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9e91b2b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9e91b2b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9e91b2b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9e91b2b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff9e91b2b50: 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
==115797==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant