jhcloos / xpdf Public

Code Issues 16 Pull requests Actions Projects Security ···

New issue

Jump to bottom

heap_buffer_overflow_in_getChar #11

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

8id93_heap_buffer_overflow_in_getChar.zip

command to reproduce

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

crash detail

```
=================================================================
==115941==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f54608ff800 at pc
0x000000750e7c bp 0x7ffdad0d6050 sp 0x7ffdad0d6048
READ of size 4 at 0x7f54608ff800 thread T0
    #0 0x750e7b in DCTStream::getChar() /home/bupt/Desktop/xpdf/xpdf/Stream.cc:2302:9
    #1 0x6899e3 in Object::streamGetChar() /home/bupt/Desktop/xpdf/xpdf/./Object.h:288:20
    #2 0x6899e3 in Lexer::getChar() /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:92:42
    #3 0x6899e3 in Lexer::getObj(Object*) /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:124:14
    #4 0x6ab867 in Parser::getObj(Object*, int, unsigned char*, CryptAlgorithm, int, int, int,
int) /home/bupt/Desktop/xpdf/xpdf/Parser.cc
    #5 0x582f60 in Gfx::go(int) /home/bupt/Desktop/xpdf/xpdf/Gfx.cc:757:13
    #6 0x581775 in Gfx::display(Object*, int) /home/bupt/Desktop/xpdf/xpdf/Gfx.cc:642:3
    #7 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
    #8 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
    #9 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
    #10 0x6a6f81 in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*),
void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:308:3
    #11 0x6af9b4 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:384:27
```

```
    #12 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
    #13 0x796d81 in main /home/bupt/Desktop/xpdf/xpdf/pdftops.cc:342:10
    #14 0x7f5463589c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #15 0x41d5d9 in _start (/home/bupt/Desktop/xpdf/xpdf/pdftops+0x41d5d9)

0x7f54608ff800 is located 0 bytes to the right of 131072-byte region
[0x7f54608df800,0x7f54608ff800)
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:2302:9 in
DCTStream::getChar()
Shadow bytes around the buggy address:
  0x0feb0c117eb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0feb0c117ec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0feb0c117ed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0feb0c117ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0feb0c117ef0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0feb0c117f00:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb0c117f10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb0c117f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb0c117f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb0c117f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0feb0c117f50: 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
==115941==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant