jhcloos / xpdf Public

<> Code   ⊙ Issues 16   Pull requests   ⊙ Actions   Projects   Security   ···

New issue

Jump to bottom

global_buffer_overflow_in_getObj #8

⊙ 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

8id65_global_buffer_overflow_in_getObj.zip

command to reproduce

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

crash detail

```
==115893==ERROR: AddressSanitizer: global-buffer-overflow on address 0x00000093aadc at pc
0x000000689c9a bp 0x7ffe79eed770 sp 0x7ffe79eed768
READ of size 1 at 0x00000093aadc thread T0
    #0 0x689c99 in Lexer::getObj(Object*) /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:132:16
    #1 0x6a8fc5 in Parser::Parser(XRef*, Lexer*, int) /home/bupt/Desktop/xpdf/xpdf/Parser.cc:33:10
    #2 0x581742 in Gfx::display(Object*, int) /home/bupt/Desktop/xpdf/xpdf/Gfx.cc:641:16
    #3 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
    #4 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
    #5 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
    #6 0x6a6f81 in Page::display(OutputDev*, double, double, int, int, int, int, int (*)(void*),
void*) /home/bupt/Desktop/xpdf/xpdf/Page.cc:308:3
    #7 0x6af9b4 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/xpdf/xpdf/PDFDoc.cc:384:27
    #8 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
    #9 0x796d81 in main /home/bupt/Desktop/xpdf/xpdf/pdftops.cc:342:10
    #10 0x7f2de419dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #11 0x41d5d9 in _start (/home/bupt/Desktop/xpdf/xpdf/pdftops+0x41d5d9)
```

```
0x00000093aadc is located 4 bytes to the left of global variable 'specialChars' defined in
'Lexer.cc:26:13' (0x93aae0) of size 256
0x00000093aadc is located 55 bytes to the right of global variable '<string literal>' defined in
'Lexer.cc:471:52' (0x93aaa0) of size 5
  '<string literal>' is ascii string 'null'
SUMMARY: AddressSanitizer: global-buffer-overflow /home/bupt/Desktop/xpdf/xpdf/Lexer.cc:132:16 in
Lexer::getObj(Object*)
Shadow bytes around the buggy address:
  0x00008011f500: f9 f9 f9 f9 00 00 04 f9 f9 f9 f9 f9 00 00 00 00
  0x00008011f510: 02 f9 f9 f9 f9 f9 f9 f9 00 00 00 f9 f9 f9 f9 f9
  0x00008011f520: 00 00 00 00 00 02 f9 f9 f9 f9 f9 f9 00 00 06 f9
  0x00008011f530: f9 f9 f9 f9 00 00 00 02 f9 f9 f9 f9 00 00 07 f9
  0x00008011f540: f9 f9 f9 f9 05 f9 f9 f9 f9 f9 f9 f9 06 f9 f9 f9
=>0x00008011f550: f9 f9 f9 f9 05 f9 f9 f9 f9 f9 f9[f9]00 00 00 00
  0x00008011f560: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x00008011f570: 00 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9
  0x00008011f580: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 00
  0x00008011f590: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x00008011f5a0: 00 00 00 00 00 00 06 f9 f9 f9 f9 f9 02 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
==115893==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant