New issue

Jump to bottom

A stack overflow in xpdf/Gfx.cc:1258 #102

Open seviezhou opened this issue on Jul 31, 2020 · 0 comments

seviezhou commented on Jul 31, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), pdf2swf (latest master fad6c2)

Command line

./pdf2swf -qq -z -o /dev/null

AddressSanitizer output

```
Error (492): Unknown operator 'P0'
=================================================================
==37915==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffea7ecce40 at pc 0x55895bd1c3a4 bp 0x7ffea7eccc30 sp 0x7ffea7eccc20
READ of size 4 at 0x7ffea7ecce40 thread T0
    #0 0x55895bd1c3a3 in Gfx::opSetFillColorN(Object*, int) xpdf/Gfx.cc:1258
    #1 0x55895bd165e5 in Gfx::go(int) xpdf/Gfx.cc:584
    #2 0x55895bd17e9f in Gfx::display(Object*, int) xpdf/Gfx.cc:556
    #3 0x55895bcb6e20 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:317
    #4 0x55895bcb7d4a in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:266
    #5 0x55895bbb95af in pdf_open /home/seviezhou/swftools/lib/pdf/pdf.cc:542
    #6 0x55895ba3b7d5 in main /home/seviezhou/swftools/src/pdf2swf.c:737
    #7 0x7f4ea43d5b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x55895ba44f09 in _start (/home/seviezhou/swftools/src/pdf2swf+0x17cf09)

Address 0x7ffea7ecce40 is located in stack of thread T0 at offset 80 in frame
    #0 0x55895bd15cef in Gfx::go(int) xpdf/Gfx.cc:561

  This frame has 2 object(s):
    [32, 48) 'obj'
    [96, 624) 'args' <== Memory access at offset 80 underflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcontext
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow xpdf/Gfx.cc:1258 Gfx::opSetFillColorN(Object*, int)
Shadow bytes around the buggy address:
  0x100054fd1970: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100054fd1980: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1
  0x100054fd1990: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100054fd19a0: f3 f3 f3 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00
  0x100054fd19b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1
=>0x100054fd19c0: f1 f1 00 00 f4 f4 f2 f2[f2]f2 00 00 00 00 00 00
  0x100054fd19d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100054fd19e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100054fd19f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100054fd1a00: 00 00 00 00 00 00 00 00 00 00 00 00 f4 f4 f3 f3
  0x100054fd1a10: f3 f3 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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==37915==ABORTING
```

POC

stack-overflow-opSetFillColorN-Gfx-1258.zip

Cvjark mentioned this issue on Jul 3

bug report swftools-pdf2swf #184

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant