New issue   Jump to bottom

A stack-buffer-overflow in VectorGraphicOutputDev.cc:1158 #106

Open   **seviezhou** opened this issue on Aug 1, 2020 · 0 comments

seviezhou commented on Aug 1, 2020

System info

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

Command line

./pdf2swf -qq -z -o /dev/null ./stack-overflow-drawGeneralImage-VectorGraphicOutputDev-1158

AddressSanitizer output

```
=================================================================
==6137==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffd2a9dcbb0 at pc 0x55fd97e56068 bp 0x7ffd2a9dc230 sp 0x7ffd2a9dc220
WRITE of size 1 at 0x7ffd2a9dcbb0 thread T0
    #0 0x55fd97e56067 in VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, Stream*, int, int, GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, 
GfxImageColorMap*) /home/seviezhou/swftools/lib/pdf/VectorGraphicOutputDev.cc:1158
    #1 0x55fd97e58db0 in VectorGraphicOutputDev::drawSoftMaskedImage(GfxState*, Object*, Stream*, int, int, GfxImageColorMap*, Stream*, int, int, GfxImageColorMap*) 
/home/seviezhou/swftools/lib/pdf/VectorGraphicOutputDev.cc:1475
    #2 0x55fd97d658a8 in Gfx::doImage(Object*, Stream*, int) xpdf/Gfx.cc:3658
    #3 0x55fd97d81d42 in Gfx::opXObject(Object*, int) xpdf/Gfx.cc:3336
    #4 0x55fd97d4f5e5 in Gfx::go(int) xpdf/Gfx.cc:584
    #5 0x55fd97d50e9f in Gfx::display(Object*, int) xpdf/Gfx.cc:556
    #6 0x55fd97cefe20 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:317
    #7 0x55fd97cf0d4a in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)(void*), void*) xpdf/Page.cc:266
    #8 0x55fd97bf6d02 in render2 /home/seviezhou/swftools/lib/pdf/pdf.cc:164
    #9 0x55fd97bf7bde in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double, double, double) /home/seviezhou/swftools/lib/pdf/pdf.cc:191
    #10 0x55fd97a75deb in main /home/seviezhou/swftools/src/pdf2swf.c:831
    #11 0x7f3da48a4b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #12 0x55fd97a7df09 in _start (/home/seviezhou/swftools/src/pdf2swf+0x17cf09)

Address 0x7ffd2a9dcbb0 is located in stack of thread T0 at offset 2240 in frame
    #0 0x55fd97e5202f in VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, Stream*, int, int, GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, 
GfxImageColorMap*) /home/seviezhou/swftools/lib/pdf/VectorGraphicOutputDev.cc:1127

  This frame has 15 object(s):
    [32, 36) 'gray'
    [96, 104) 'x1'
    [160, 168) 'y1'
    [224, 232) 'x2'
    [288, 296) 'y2'
    [352, 360) 'x3'
    [416, 424) 'y3'
    [480, 488) 'x4'
    [544, 552) 'y4'
    [608, 620) 'rgb'
    [672, 752) 'color_transform'
    [800, 1824) 'pal'
    [1856, 1860) 'pixBuf'
    [1920, 1928) 'buf'
    [1984, 2240) 'pal' <== Memory access at offset 2240 overflows 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 /home/seviezhou/swftools/lib/pdf/VectorGraphicOutputDev.cc:1158 VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, 
Stream*, int, int, GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, GfxImageColorMap*)
Shadow bytes around the buggy address:
  0x100025533920: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100025533930: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100025533940: 00 00 f2 f2 f2 f2 04 f4 f4 f4 f2 f2 f2 f2 00 f4
  0x100025533950: f4 f4 f2 f2 f2 f2 00 00 00 00 00 00 00 00 00 00
  0x100025533960: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x100025533970: 00 00 00 00 00 00[f3]f3 f3 f3 f3 f3 f3 f3 00 00
  0x100025533980: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100025533990: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000255339a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000255339b0: 00 00 f1 f1 f1 f1 04 f4 f4 f4 f2 f2 f2 f2 04 f4
  0x1000255339c0: f4 f4 f2 f2 f2 f2 00 00 f4 f4 f2 f2 f2 f2 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
==6137==ABORTING
```

POC

stack-overflow-drawGeneralImage-VectorGraphicOutputDev-1158.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