Bug 701786 - stack-buffer-overflow at base/gsbitops.c:677 in bytes_copy_rectangle

Status: RESOLVED FIXED
Alias: None
Product: Ghostscript
Component: Valgrind/AddressSanitizer (show other bugs)
Version: master
Hardware: PC Linux
Importance: P4 normal
Assignee: Ray Johnston
URL:
Keywords:
Depends on:
Blocks:

Reported: 2019-10-26 05:30 UTC by Suhwan
Modified: 2019-10-28 02:53 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (3.38 KB, application/pdf) 2019-10-26 05:30 UTC, Suhwan	Details
Add an attachment (proposed patch, testcase, etc.)	

Note
You need to log in before you can comment on or make changes to this bug.

Suhwan 2019-10-26 05:30:07 UTC Description

Created attachment 18370 [details]
poc

Hello.

I found a stack-buffer-overflow bug in GhostScript.

Please confirm.

Thanks.

OS: Ubuntu 18.04 64bit

Steps to reproduce:
1. Download the .POC files.
2. Compile the source code with ASan.
3. Run following cmd.
$ gs -r652 -dFitPage -sOutputFile=tmp -sDEVICE=jetp3852 $PoC

Here's ASAN report.

```
=================================================================
==37765==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fff22447700
at pc 0x0000004a18cc bp 0x7fff22445230 sp 0x7fff224449e0
WRITE of size 5604 at 0x7fff22447700 thread T0
    #0 0x4a18cb in __interceptor_memcpy.part.40 (gs+0x4a18cb)
    #1 0x227267d in bytes_copy_rectangle ghostpdl/./base/gsbitops.c:677:9
    #2 0x2bb09f9 in gx_get_bits_copy ghostpdl/./base/gdevdgbr.c:311:13
    #3 0x2bd0d46 in mem_get_bits_rectangle ghostpdl/./base/gdevmem.c:639:16
    #4 0x14d225b in clist_get_bits_rectangle ghostpdl/./base/gxclread.c:639:16
    #5 0x1596512 in clist_get_bits_rect_mt ghostpdl/./base/gxclthrd.c:860:13
    #6 0x2bae551 in gx_default_get_bits ghostpdl/./base/gdevdgbr.c:54:12
    #7 0x13f6b97 in gdev_prn_get_bits ghostpdl/./base/gdevprn.c:1687:16
    #8 0x13f6b97 in gdev_prn_copy_scan_lines ghostpdl/./base/gdevprn.c:1712
    #9 0x1f2ee25 in jetp3852_print_page ghostpdl/./devices/gdev3852.c:82:13
    #10 0x13f07d9 in gx_default_print_page_copies ghostpdl/./base/gdevprn.c:1231:12
    #11 0x13ef028 in gdev_prn_output_page_aux ghostpdl/./base/gdevprn.c:1133:27
    #12 0x22b6f20 in gs_output_page ghostpdl/./base/gsdevice.c:212:17
    #13 0x3054b9f in zoutputpage ghostpdl/./psi/zdevice.c:416:12
    #14 0x2e8bdb6 in interp ghostpdl/./psi/interp.c:1300:28
    #15 0x2e8bdb6 in gs_call_interp ghostpdl/./psi/interp.c:520
    #16 0x2e8bdb6 in gs_interpret ghostpdl/./psi/interp.c:477
    #17 0x2e3f451 in gs_main_interpret ghostpdl/./psi/imain.c:253:12
    #18 0x2e3f451 in gs_main_run_string_end ghostpdl/./psi/imain.c:791
    #19 0x2e3f451 in gs_main_run_string_with_length ghostpdl/./psi/imain.c:735
    #20 0x2e548f0 in run_string ghostpdl/./psi/imainarg.c:1117:12
    #21 0x2e548f0 in runarg ghostpdl/./psi/imainarg.c:1086
    #22 0x2e5302a in argproc ghostpdl/./psi/imainarg.c:1008:16
    #23 0x2e479f7 in gs_main_init_with_args01 ghostpdl/./psi/imainarg.c:241:24
    #24 0x2e539d0 in gs_main_init_with_args ghostpdl/./psi/imainarg.c:288:16
    #25 0x57b86f in main ghostpdl/./psi/gs.c:95:16
    #26 0x7fab326b1b96 in __libc_start_main /build/glibc-OTsEL5/glibc-
2.27/csu/../csu/libc-start.c:310
    #27 0x482e79 in _start (gs+0x482e79)

Address 0x7fff22447700 is located in stack of thread T0 at offset 800 in frame
    #0 0x1f2ea1f in jetp3852_print_page ghostpdl/./devices/gdev3852.c:61

  This frame has 2 object(s):
    [32, 800) 'data' (line 69)
    [928, 1216) 'plane_data' (line 70) <== Memory access at offset 800 partially
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 (gs+0x4a18cb) in
__interceptor_memcpy.part.40
Shadow bytes around the buggy address:
  0x100064480e90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100064480ea0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100064480eb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100064480ec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100064480ed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x100064480ee0:[f2]f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2
  0x100064480ef0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100064480f00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100064480f10: 00 00 00 00 f3 f3 f3 f3 f3 f3 f3 f3 00 00 00 00
  0x100064480f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100064480f30: 00 00 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
  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
==37765==ABORTING
```

Ray Johnston 2019-10-28 02:53:37 UTC **Comment 1**

```
Fixed by detecting the invalid byte count that can be caused by wide pages
or high resolutions. A badly designed 'contrib' device, so just detect that
the number of bytes needed will exceed what the device can handle, and throw
an error. With the test conditions, the result is now:

GPL Ghostscript GIT PRERELEASE 9.51: invalid resolution and/or width gives
line_size = 5604, max. is 768
Error: /rangecheck in --showpage--
    then following the usual error printout:
GPL Ghostscript GIT PRERELEASE 9.51: Unrecoverable error, exit code 1

Fixed by commit 93cb0c0adbd9bcfefd021d59c472388f67d3300d
```