Bug 701795 - Segmentation fault at base/gxblend.c:3091 in compose_group_nonknockout_nonblend_isolated_allmask_common

Status: RESOLVED FIXED
Alias: None
Product: Ghostscript
Component: Transparency (show other bugs)
Version: master
Hardware: PC Linux
Importance: P4 normal
Assignee: Michael Vrhel
URL:
Keywords:
Depends on:
Blocks:

Reported: 2019-10-26 08:12 UTC by Suhwan
Modified: 2019-10-28 22:18 UTC (History)
CC List: 0 users
See Also:
Customer:
Word Size: ---

Attachments	
poc (12.96 KB, application/pdf) 2019-10-26 08:12 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 08:12:44 UTC — Description

Created attachment 18379 [details]
poc

Hello.

I found a Segmentation fault 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 -sOutputFile=tmp -sDEVICE=eplmono $PoC
```

Here's ASAN report.

```
=================================================================
==384==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc
0x000000c257b4 bp 0x62900006e444 sp 0x7fff87ad9590 T0)
==384==The signal is caused by a READ memory access.
==384==Hint: address points to the zero page.
    #0 0xc257b3 in compose_group_nonknockout_nonblend_isolated_allmask_common
ghostpdl/./base/gxblend.c:3091:36
    #1 0xbf91f0 in do_compose_group ghostpdl/./base/gxblend.c:3509:5
    #2 0xbf91f0 in pdf14_compose_group ghostpdl/./base/gxblend.c:4302
    #3 0xd1cb2c in pdf14_pop_transparency_group ghostpdl/./base/gdevp14.c:1609:13
    #4 0xcda8b4 in pdf14_end_transparency_group ghostpdl/./base/gdevp14.c:5154:12
    #5 0xd22d9a in gx_update_pdf14_compositor ghostpdl/./base/gdevp14.c:4643:20
    #6 0x14c9a8f in apply_create_compositor ghostpdl/./base/gxclrast.c:2999:12
    #7 0x14c9a8f in execute_compositor_queue ghostpdl/./base/gxclrast.c:386
    #8 0x14a7e0e in clist_playback_band ghostpdl/./base/gxclrast.c:1623:52
    #9 0x14cd97b in clist_playback_file_bands ghostpdl/./base/gxclread.c:920:16
    #10 0x14d5c63 in clist_render_rectangle ghostpdl/./base/gxclread.c:854:16
    #11 0x14d413f in clist_rasterize_lines ghostpdl/./base/gxclread.c:743:20
    #12 0x14d2154 in clist_get_bits_rectangle ghostpdl/./base/gxclread.c:632:12
    #13 0x1596512 in clist_get_bits_rect_mt ghostpdl/./base/gxclthrd.c:860:13
    #14 0x2bae551 in gx_default_get_bits ghostpdl/./base/gdevdgbr.c:54:12
    #15 0xd4f187 in pdf14_clist_create_compositor ghostpdl/./base/gdevp14.c:8711:20
    #16 0xcc7569 in send_pdf14trans ghostpdl/./base/gdevp14.c:7737:12
    #17 0xbb43ea in gs_gstate_update_pdf14trans2 ghostpdl/./base/gstrans.c:168:12
    #18 0xbb43ea in gs_gstate_update_pdf14trans ghostpdl/./base/gstrans.c:192
    #19 0xbb43ea in gs_pop_pdf14trans_device ghostpdl/./base/gstrans.c:832
    #20 0x2e8bdb6 in interp ghostpdl/./psi/interp.c:1300:28
    #21 0x2e8bdb6 in gs_call_interp ghostpdl/./psi/interp.c:520
    #22 0x2e8bdb6 in gs_interpret ghostpdl/./psi/interp.c:477
    #23 0x2e3f451 in gs_main_interpret ghostpdl/./psi/imain.c:253:12
    #24 0x2e3f451 in gs_main_run_string_end ghostpdl/./psi/imain.c:791
    #25 0x2e3f451 in gs_main_run_string_with_length ghostpdl/./psi/imain.c:735
    #26 0x2e548f0 in run_string ghostpdl/./psi/imainarg.c:1117:12
    #27 0x2e548f0 in runarg ghostpdl/./psi/imainarg.c:1086
    #28 0x2e5302a in argproc ghostpdl/./psi/imainarg.c:1008:16
    #29 0x2e479f7 in gs_main_init_with_args01 ghostpdl/./psi/imainarg.c:241:24
    #30 0x2e539d0 in gs_main_init_with_args ghostpdl/./psi/imainarg.c:288:16
    #31 0x57b86f in main ghostpdl/./psi/gs.c:95:16
    #32 0x7fbc119a3b96 in __libc_start_main /build/glibc-OTsEL5/glibc-
2.27/csu/../csu/libc-start.c:310
    #33 0x482e79 in _start (gs+0x482e79)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ghostpdl/./base/gxblend.c:3091:36 in
compose_group_nonknockout_nonblend_isolated_allmask_common
==384==ABORTING
```

Ken Sharp 2019-10-26 08:43:30 UTC — Comment 1

SHA1 4b9e86a33b237740df682369300f1a9507dc63c5 exhibits this, assigning to Michael as it appears to be somethign to do with transparency.

Suhwan 2019-10-26 09:27:41 UTC — Comment 2

I built gs on git commit commit 4b9e86a33b237740df682369300f1a9507dc63c5
with gcc compiler and used "make sanitize"

```
GPL Ghostscript GIT PRERELEASE 9.51 (2019-10-15)
Copyright (C) 2019 Artifex Software, Inc.  All rights reserved.
This software is supplied under the GNU AGPLv3 and comes with NO WARRANTY:
see the file COPYING for details.
   **** Error:  An error occurred while reading an XREF table.
   **** The file has been damaged.  This may have been caused
   **** by a problem while converting or transfering the file.
   **** Ghostscript will attempt to recover the data.
   **** However, the output may be incorrect.
Processing pages 1 through 1.
Page 1
   **** Error: stream Length incorrect.
               Output may be incorrect.
```

```
warning: ignoring zlib error: incorrect data check
   **** Error: stream Length incorrect.
               Output may be incorrect.
   **** Error: stream Length incorrect.
               Output may be incorrect.

   **** Error: File has insufficient data for an image.
               Output may be incorrect.
ASAN:DEADLYSIGNAL
=================================================================
==6325==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc
0x5587e93ceb3f bp 0x7ffd3e5f3610 sp 0x7ffd3e5f35b0 T0)
==6325==The signal is caused by a READ memory access.
==6325==Hint: address points to the zero page.
    #0 0x5587e93ceb3e in compose_group_nonknockout_nonblend_isolated_allmask_common
base/gxblend.c:3091
    #1 0x5587e93d11bc in do_compose_group base/gxblend.c:3509
    #2 0x5587e93d6436 in pdf14_compose_group base/gxblend.c:4302
    #3 0x5587e93f0e72 in pdf14_pop_transparency_group base/gdevp14.c:1609
    #4 0x5587e941076d in pdf14_end_transparency_group base/gdevp14.c:5154
    #5 0x5587e93b1153 in gx_end_transparency_group base/gstrans.c:437
    #6 0x5587e940c3d7 in gx_update_pdf14_compositor base/gdevp14.c:4643
    #7 0x5587e940ca27 in pdf14_create_compositor base/gdevp14.c:4730
    #8 0x5587e97a336e in apply_create_compositor base/gxclrast.c:2999
    #9 0x5587e9780dd9 in execute_compositor_queue base/gxclrast.c:386
    #10 0x5587e97914db in clist_playback_band base/gxclrast.c:1631
    #11 0x5587e97b0468 in clist_playback_file_bands base/gxclread.c:920
    #12 0x5587e97afc45 in clist_render_rectangle base/gxclread.c:854
    #13 0x5587e97aec1b in clist_rasterize_lines base/gxclread.c:743
    #14 0x5587e97ada2a in clist_get_bits_rectangle base/gxclread.c:632
    #15 0x5587e9816785 in clist_get_bits_rect_mt base/gxclthrd.c:845
    #16 0x5587ea25b660 in gx_default_get_bits base/gdevdgbr.c:54
    #17 0x5587e943028e in pdf14_clist_create_compositor base/gdevp14.c:8711
    #18 0x5587e9427e20 in send_pdf14trans base/gdevp14.c:7737
    #19 0x5587e93ae151 in gs_gstate_update_pdf14trans2 base/gstrans.c:168
    #20 0x5587e93ae332 in gs_gstate_update_pdf14trans base/gstrans.c:192
    #21 0x5587e93b4e4e in gs_pop_pdf14trans_device base/gstrans.c:832
    #22 0x5587ea53505c in zpoppdf14devicefilter psi/ztrans.c:551
    #23 0x5587ea38cfd3 in do_call_operator psi/interp.c:86
    #24 0x5587ea396752 in interp psi/interp.c:1300
    #25 0x5587ea38eb20 in gs_call_interp psi/interp.c:520
    #26 0x5587ea38e1c5 in gs_interpret psi/interp.c:477
    #27 0x5587ea36271c in gs_main_interpret psi/imain.c:253
    #28 0x5587ea365bd1 in gs_main_run_string_end psi/imain.c:791
    #29 0x5587ea365596 in gs_main_run_string_with_length psi/imain.c:735
    #30 0x5587ea365508 in gs_main_run_string psi/imain.c:716
    #31 0x5587ea3721cc in run_string psi/imainarg.c:1117
    #32 0x5587ea371f6f in runarg psi/imainarg.c:1086
    #33 0x5587ea3717ee in argproc psi/imainarg.c:1008
    #34 0x5587ea36bfba in gs_main_init_with_args01 psi/imainarg.c:241
    #35 0x5587ea36c41e in gs_main_init_with_args psi/imainarg.c:288
    #36 0x5587ea37794e in psapi_init_with_args psi/psapi.c:272
    #37 0x5587ea546f6d in gsapi_init_with_args psi/iapi.c:148
    #38 0x5587e9118598 in main psi/gs.c:95
    #39 0x7f0c4217ab96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #40 0x5587e9118339 in _start (gs_gcc_asan+0x36b339)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV base/gxblend.c:3091 in
compose_group_nonknockout_nonblend_isolated_allmask_common
```

Michael Vrhel **2019-10-28 22:18:39 UTC** **Comment 3**

Fixed with

https://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=7870f4951bcc6a153f317e3439e14d0e929fd231