Bug 701822 - Segmentation fault at psi/iname.c:296 in names_index_ref

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

Reported: 2019-11-01 07:05 UTC by Suhwan
Modified: 2021-09-11 12:56 UTC (History)
CC List: 2 users (show)
See Also:
Customer:
Word Size: ---

Attachments	
poc (48.10 KB, application/postscript) 2019-11-01 07:05 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 2019-11-01 07:05:37 UTC — Description

Created attachment 18409 [details]
poc

Hello

I found a Segmentation fault bug in GhostScript.
Please confirm.
Thanks.

OS: Ubuntu 18.04 64bit
Version: commit 9c196bb7f6873b4fe43a649fc87cba363c6af8e5

Steps to reproduce:
1. Download the .POC files.
2. Compile the source code with "make sanitize" using gcc.
3. Run following cmd.

```
gs -dBATCH -dNOPAUSE -sOutputFile=tmp -sDEVICE=txtwrite $PoC
```

Here's ASAN report.

```
==14954==ERROR: AddressSanitizer: SEGV on unknown address 0x62f004004478 (pc
0x55ae28a987f9 bp 0x7ffebd4868c0 sp 0x7ffebd4868a0 T0)
==14954==The signal is caused by a READ memory access.
    #0 0x55ae28a987f8 in names_index_ref psi/iname.c:296
    #1 0x55ae28a0731a in gs_font_map_glyph_by_dict psi/zbfont.c:184
    #2 0x55ae28a08248 in gs_font_map_glyph_to_unicode psi/zbfont.c:278
    #3 0x55ae281915de in get_unicode devices/vector/gdevtxtw.c:1694
    #4 0x55ae28193baf in txtwrite_process_cmap_text devices/vector/gdevtxtw.c:1893
    #5 0x55ae28198142 in textw_text_process devices/vector/gdevtxtw.c:2189
    #6 0x55ae2849fd49 in gs_text_process base/gstext.c:596
    #7 0x55ae28a14ec7 in op_show_continue_pop psi/zchar.c:696
    #8 0x55ae28a0f8ec in zshow psi/zchar.c:78
    #9 0x55ae2897ea2f in do_call_operator psi/interp.c:86
    #10 0x55ae289881ae in interp psi/interp.c:1300
    #11 0x55ae2898057c in gs_call_interp psi/interp.c:520
    #12 0x55ae2897fc21 in gs_interpret psi/interp.c:477
    #13 0x55ae28954178 in gs_main_interpret psi/imain.c:253
    #14 0x55ae2895762d in gs_main_run_string_end psi/imain.c:791
    #15 0x55ae28956ff2 in gs_main_run_string_with_length psi/imain.c:735
    #16 0x55ae28956f64 in gs_main_run_string psi/imain.c:716
    #17 0x55ae28963c28 in run_string psi/imainarg.c:1117
    #18 0x55ae289639cb in runarg psi/imainarg.c:1086
    #19 0x55ae2896324a in argproc psi/imainarg.c:1008
    #20 0x55ae2895da16 in gs_main_init_with_args01 psi/imainarg.c:241
    #21 0x55ae2895de7a in gs_main_init_with_args psi/imainarg.c:288
    #22 0x55ae289693aa in psapi_init_with_args psi/psapi.c:272
    #23 0x55ae28b389c9 in gsapi_init_with_args psi/iapi.c:148
    #24 0x55ae277096b8 in main psi/gs.c:95
    #25 0x7fd8636a3b96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #26 0x55ae27709459 in _start (gs+0x36c459)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV psi/iname.c:296 in names_index_ref
```

Ken Sharp 2019-11-03 15:40:00 UTC — Comment 1

I've tried the specified SHA and the current HEAD (366ad48d076c1aa4c8f83c65011258a04e348207) on 64-bit Ubuntu using make sanitize, and cannto reproduce this problem.

I also tried 64-bit WIndows and 32-bit WIndows, debug and release versions of each, without any problems.

In short, I cannot reproduce this on any system.

Alex Cherepanov 2019-11-04 15:26:55 UTC — Comment 2

I can easily reproduce this SEGV by running the current gs, debug or release, as described in this bug report.

Ken Sharp 2019-11-04 15:40:47 UTC — Comment 3

(In reply to Alex Cherepanov from comment #2)
> I can easily reproduce this SEGV by running the current gs, debug or
> release, as described in this bug report.

Hmm, oddly today it does indeed reproduce, on Linux, no idea why it wouldn't yesterday.

Ken Sharp 2019-11-05 08:52:20 UTC — Comment 4

I believe this is fixed in commit 407c98a38c3a6ac1681144ed45cc2f4fc374c91f