Bug 701821 - Segmentation fault at tiff//libtiff/tif_dirinfo.c:513 in TIFFFindField

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

Reported: 2019-11-01 07:01 UTC by Suhwan
Modified: 2021-10-30 08:16 UTC (History)
CC List: 1 user (show)
See Also:
Customer:
Word Size: ---

Attachments	
poc (99.59 KB, application/postscript) 2019-11-01 07:01 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 07:01:55 UTC — Description

Created attachment 18407 [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=tiffsep $PoC
```

Here's ASAN report.

```
==9722==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000400 (pc
0x5622f5d5279a bp 0x7ffeec399370 sp 0x7ffeec399270 T0)
==9722==The signal is caused by a READ memory access.
==9722==Hint: address points to the zero page.
    #0 0x5622f5d52799 in TIFFFindField tiff//libtiff/tif_dirinfo.c:513
    #1 0x5622f5d45fce in OkToChangeTag tiff//libtiff/tif_dir.c:762
    #2 0x5622f5d4685a in TIFFVSetField tiff//libtiff/tif_dir.c:853
    #3 0x5622f5d462e6 in TIFFSetField tiff//libtiff/tif_dir.c:798
    #4 0x5622f5e343c5 in tiff_set_fields_for_printer devices/gdevtifs.c:380
    #5 0x5622f604f45a in tiffsep_print_page devices/gdevtsep.c:2390
    #6 0x5622f5bf61c2 in gx_default_print_page_copies base/gdevprn.c:1231
    #7 0x5622f5bf5b91 in gdev_prn_output_page_aux base/gdevprn.c:1133
    #8 0x5622f5bf5e5a in gdev_prn_output_page_seekable base/gdevprn.c:1175
    #9 0x5622f62d371a in gs_output_page base/gsdevice.c:212
    #10 0x5622f6932cc3 in zoutputpage psi/zdevice.c:416
    #11 0x5622f684fa2f in do_call_operator psi/interp.c:86
    #12 0x5622f68591ae in interp psi/interp.c:1300
    #13 0x5622f685157c in gs_call_interp psi/interp.c:520
    #14 0x5622f6850c21 in gs_interpret psi/interp.c:477
    #15 0x5622f6825178 in gs_main_interpret psi/imain.c:253
    #16 0x5622f682862d in gs_main_run_string_end psi/imain.c:791
    #17 0x5622f6827ff2 in gs_main_run_string_with_length psi/imain.c:735
    #18 0x5622f6827f64 in gs_main_run_string psi/imain.c:716
    #19 0x5622f6834c28 in run_string psi/imainarg.c:1117
    #20 0x5622f68349cb in runarg psi/imainarg.c:1086
    #21 0x5622f683424a in argproc psi/imainarg.c:1008
    #22 0x5622f682ea16 in gs_main_init_with_args01 psi/imainarg.c:241
    #23 0x5622f682ee7a in gs_main_init_with_args psi/imainarg.c:288
    #24 0x5622f683a3aa in psapi_init_with_args psi/psapi.c:272
    #25 0x5622f6a099c9 in gsapi_init_with_args psi/iapi.c:148
    #26 0x5622f55da6b8 in main psi/gs.c:95
    #27 0x7f2d4330eb96 in __libc_start_main (/lib/x86_64-linux-
gnu/libc.so.6+0x21b96)
    #28 0x5622f55da459 in _start (gs+0x36c459)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV tiff//libtiff/tif_dirinfo.c:513 in TIFFFindField
```

Ken Sharp 2019-11-01 10:27:55 UTC — Comment 1

Fixed in commit aadb53eb834b3def3ef68d78865ff87a68901804