Bug 701796 - Segmentation fault at devices/gdevclj.c:269 in clj_media_size

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

Reported: 2019-10-26 08:19 UTC by Suhwan
Modified: 2019-10-26 16:15 UTC (History)
CC List: 1 user (show)
See Also:
Customer:
Word Size: ---

Attachments	
poc (73.21 KB, application/pdf) 2019-10-26 08:19 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 08:19:21 UTC — Description

Created attachment 18380 [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  -dUseCIEColor -dFIXEDMEDIA -sOutputFile=tmp -sDEVICE=cljet5 $PoC
```

Here's ASAN report.

```
=================================================================
==6709==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc
0x000001e734f0 bp 0x7ffceba057d0 sp 0x7ffceba056e0 T0)
==6709==The signal is caused by a READ memory access.
==6709==Hint: address points to the zero page.
    #0 0x1e734ef in clj_media_size ghostpdl/./devices/gdevclj.c:269:55
    #1 0x1e7288d in clj_put_params ghostpdl/./devices/gdevclj.c:289:45
    #2 0x1452571 in default_subclass_put_params ghostpdl/./base/gdevsclass.c:235:16
    #3 0x22e11dc in gs_putdeviceparams ghostpdl/./base/gsdparam.c:1008:12
    #4 0x305537e in zputdeviceparams ghostpdl/./psi/zdevice.c:470:12
    #5 0x2e8e638 in interp ghostpdl/./psi/interp.c:1674:40
    #6 0x2e8e638 in gs_call_interp ghostpdl/./psi/interp.c:520
    #7 0x2e8e638 in gs_interpret ghostpdl/./psi/interp.c:477
    #8 0x2e383f9 in gs_main_interpret ghostpdl/./psi/imain.c:253:12
    #9 0x2e383f9 in gs_run_init_file ghostpdl/./psi/imain.c:707
    #10 0x2e383f9 in gs_main_init2aux ghostpdl/./psi/imain.c:301
    #11 0x2e38dff in gs_main_init2 ghostpdl/./psi/imain.c:338:12
    #12 0x2e542bc in runarg ghostpdl/./psi/imainarg.c:1072:16
    #13 0x2e5302a in argproc ghostpdl/./psi/imainarg.c:1008:16
    #14 0x2e479f7 in gs_main_init_with_args01 ghostpdl/./psi/imainarg.c:241:24
    #15 0x2e539d0 in gs_main_init_with_args ghostpdl/./psi/imainarg.c:288:16
    #16 0x57b86f in main ghostpdl/./psi/gs.c:95:16
    #17 0x7f706dae4b96 in __libc_start_main /build/glibc-OTsEL5/glibc-
2.27/csu/../csu/libc-start.c:310
    #18 0x482e79 in _start (gs+0x482e79)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ghostpdl/./devices/gdevclj.c:269:55 in
clj_media_size
==6709==ABORTING
```

Ken Sharp 2019-10-26 14:00:13 UTC — Comment 1

It appears that this line:

```
    if ( (param_read_float_array(plist, "HWResolution", &fres) == 0) &&
          !is_supported_resolution(fres.data) )
        return_error(gs_error_rangecheck);
```

isn't catering for param_read_float_array() returning an error, which it does. Its apparently unable to read a HWResolution from the plist. This leads to a later divide-by-zero error.

```
        mediasize[0] = ((float)hwsize.data[0]) * 72 / fres.data[0];
```

Altering this line to:

```
    if ( param_read_float_array(plist, "HWResolution", &fres) != 0 ||
          !is_supported_resolution(fres.data) )
        return_error(gs_error_rangecheck);
```

throws an error instead. Not obvious to me if this should be an error though.

Ken Sharp 2019-10-26 16:15:48 UTC — Comment 2

Fixed (at least, it no longer seg faults) in commit 2c2dc335c212750e0fb8ae157063bc06cafa8d3e

I'm not absolutely certain this is the best solution, but a crash is bad, and this prevents that happening.