darktable - Bug #11672

amaze demosaic: heap buffer overflow

07/20/2017 07:15 PM - FI Fr

Status:	New	**Start date:**	07/20/2017
Priority:	Medium	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Affected Version:	git master branch	**bitness:**	64-bit
System:	other GNU/Linux	**hardware architecture:**	amd64/x86

Description

└> env ASAN_OPTIONS=new_delete_type_mismatch=0 darktable

(darktable:25310): GLib-GObject-CRITICAL **: g_object_set_data: assertion 'G_IS_OBJECT (object)' failed

(darktable:25310): Gtk-CRITICAL **: gtk_widget_get_has_tooltip: assertion 'GTK_IS_WIDGET (widget)' failed
===
25310ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f353ca0604c at pc 0x7f356b12183d bp 0x7f353d1f66b0 sp 0x7f353d1f66a8
READ of size 16 at 0x7f353ca0604c thread T98
25310AddressSanitizer: while reporting a bug found another one. Ignoring.
#0 0x7f356b12183c in amaze_demosaic_RT._omp_fn.0 /usr/lib/gcc/x86_64-pc-linux-gnu/7.1.0/include/xmmintrin.h:934
#1 0x7f3597339892 in gomp_thread_start /home/sourcemage/build_directory/gcc-7.1.0/libgomp/team.c:120
#2 0x7f359d6ef363 in start_thread (/lib/libpthread.so.0+0x7363)
#3 0x7f359d45ea8e in __clone (/lib/libc.so.6+0xdda8e)

0x7f353ca06050 is located 0 bytes to the right of 4741200-byte region [0x7f353c580800,0x7f353ca06050)
allocated by thread T11 (worker res 1) here:
#0 0x7f359e324c94 in __interceptor_posix_memalign /home/sourcemage/build_directory/gcc-7.1.0/libsanitizer/asan/asan_malloc_linux.cc:134
#1 0x7f359da49d50 in dt_alloc_align /home/florian/repos/darktable/src/common/darktable.c:1141
#2 0x7f356b10c35b in process /home/florian/repos/darktable/src/iop/demosaic.c:1722
#3 0x7f359dba8c86 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:1527
#4 0x7f359dba8044 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:702
#5 0x7f359dba8044 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:702
#6 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#7 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#8 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#9 0x7f359dba8044 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:702
#10 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#11 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#12 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#13 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#14 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#15 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#16 0x7f359dba8044 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:702
#17 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#18 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#19 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#20 0x7f359dba8044 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:702
#21 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#22 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#23 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#24 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#25 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#26 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#27 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583
#28 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583

```
#29 0x7f359dba7347 in dt_dev_pixelpipe_process_rec /home/florian/repos/darktable/src/develop/pixelpipe_hb.c:583

Thread T98 created by T11 (worker res 1) here:
#0 0x7f359e2a4cbe in __interceptor_pthread_create
/home/sourcemage/build_directory/gcc-7.1.0/libsanitizer/asan/asan_interceptors.cc:243
#1 0x7f359733a6b0 in gomp_team_start /home/sourcemage/build_directory/gcc-7.1.0/libgomp/team.c:817
#2 0x7f3597335a8f in GOMP_parallel /home/sourcemage/build_directory/gcc-7.1.0/libgomp/parallel.c:167
#3 0x3ed921823dcccccc  (<unknown module>)

Thread T11 (worker res 1) created by T0 here:
#0 0x7f359e2a4cbe in __interceptor_pthread_create
/home/sourcemage/build_directory/gcc-7.1.0/libsanitizer/asan/asan_interceptors.cc:243
#1 0x7f359da5ffb0 in dt_pthread_create /home/florian/repos/darktable/src/common/dtpthread.c:65
#2 0x7f359db4e7e1 in dt_control_init /home/florian/repos/darktable/src/control/control.c:70
#3 0x7f359da4ea64 in dt_init /home/florian/repos/darktable/src/common/darktable.c:855
 #4 0x4008f5 in main /home/florian/repos/darktable/src/main.c:64
#5 0x7f359d3a1349 in __libc_start_main (/lib/libc.so.6+0x20349)

SUMMARY: AddressSanitizer: heap-buffer-overflow /usr/lib/gcc/x86_64-pc-linux-gnu/7.1.0/include/xmmintrin.h:934 in
amaze_demosaic_RT._omp_fn.0
Shadow bytes around the buggy address:
0x0fe727938bb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fe727938bc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fe727938bd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fe727938be0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fe727938bf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fe727938c00: 00 00 00 00 00 00 00 00[00]fa fa fa fa fa fa
0x0fe727938c10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe727938c20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe727938c30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe727938c40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fe727938c50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
25310ABORTING

commit hash is 075d6fb12060355d33c0c005154d3fe5de713d54
```

History

#1 - 07/20/2017 07:17 PM - Roman Lebedev

- Priority changed from Low to Medium

- Subject changed from heap buffer overflow when entering darkroom to amaze demosaic: heap buffer overflow

#2 - 07/20/2017 08:00 PM - Fl Fr

- File DSC_5017.NEF.xmp added

Files

DSC_5017.NEF	27.7 MB	07/20/2017	Fl Fr
DSC_5017.NEF.xmp	4.72 KB	07/20/2017	Fl Fr