darktable - Bug #12461

segmentation fault at high zoom level and the equalizer module

12/12/2018 12:15 AM - Heiko Bauke

Status:	Fixed	**Start date:**	12/12/2018
Priority:	Medium	**Due date:**	
Assignee:	Pascal Obry	**% Done:**	100%
Category:	Darkroom	**Estimated time:**	0.00 hour
Target version:	2.6.0		
Affected Version:	git master branch	**bitness:**	64-bit
System:	Ubuntu	**hardware architecture:**	amd64/x86

Description

Working in the darkroom tab I get always a segmentation fault when the following two conditions are met:

- zoom level is at 400% or above,
- at least one instance of the equalizer module is active.

Associated revisions

Revision 0a33be3c - 12/14/2018 09:03 PM - Heiko Bauke

equalizer: fix bug #12461 and fix radius in tiling_callback

Revision 3f9f754d - 12/15/2018 12:43 AM - Pascal Obry

Merge pull request #1902 from rabauke/my_atrous

equalizer: fix bug #12461 and fix radius in tiling_callback

History

#1 - 12/12/2018 12:40 AM - Heiko Bauke

I created a debug build and attached a debugger to darktable. The segmentation fault comes from the function weight_sse2 in the file atrours.c. The pointer argument c1 points to an invalid address, this means that the variable px, which is passed as c1 to the function weight_sse2, is invalid. The root cause for this issue is somewhat difficult to debug due to the many source manipulating macros.

#2 - 12/12/2018 03:12 AM - Heiko Bauke

I think cases where 2*mult>=height or 2*mult>=width are not treated correctly in the functions eaw_decompose and eaw_decompose_sse2, which causes the segmentation fault.

#3 - 12/14/2018 04:14 PM - Pascal Obry

I can't reproduce. Is that with out without OpenCL.

#4 - 12/14/2018 07:17 PM - Aurélien PIERRE

It should be without OpenCL, since the SSE2 function are affected.

#5 - 12/14/2018 07:22 PM - Pascal Obry

Indeed, I missed this in the comment. I'll try again.

#6 - 12/14/2018 07:42 PM - Pascal Obry

- Priority changed from Low to Medium

I can reproduce for zoom level > 400%, it is immediate as soon as I pass the zoom to 800%.

This will probably take someone knowing well this part of the code and SSE2.

#7 - 12/14/2018 07:52 PM - Pascal Obry

Same issue in non SS2 path:

```
(gdb) bt
#0  0x00007fffdc073f5c in weight
    (weight=<synthetic pointer>, sharpen=<optimized out>, c2=0x7fff71bee040, c1=0x7fff71bdfc70)
    at /home/obry/dev/builds/darktable/build/src/src/iop/atrous.c:168
#1  0x00007fffdc073f5c in eaw_decompose._omp_fn
    (out=<optimized out>, in=<optimized out>, detail=<optimized out>, scale=<optimized out>, sharpen=<optimize
d out>, width=<optimized out>, height=<optimized out>) at /home/obry/dev/builds/darktable/build/src/src/iop/at
rous.c:420
#2  0x00007ffff792a73e in  () at /usr/lib/x86_64-linux-gnu/libgomp.so.1
#3  0x00007ffff7acffa3 in start_thread (arg=<optimized out>)
    at pthread_create.c:486
#4  0x00007ffff7be288f in clone ()
    at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95
```

This may be easier to debug. It is in the same part of the code but for standard CPU path.

#8 - 12/14/2018 09:47 PM - Heiko Bauke

I opened a pull request to fix this issue.

#9 - 12/15/2018 12:57 AM - Pascal Obry

- % Done changed from 0 to 100

- Status changed from New to Fixed

- Assignee set to Pascal Obry

Thanks, this is now integrated.