darktable - Bug #11047

segfault due to double free while importing stuff

06/07/2016 07:05 PM - Jan Kundrát

Status:	New	**Start date:**	06/07/2016
Priority:	Medium	**Due date:**	
Assignee:		**% Done:**	0%
Category:	General	**Estimated time:**	0.00 hour
Target version:			
Affected Version:	git development version	**bitness:**	64-bit
System:	other GNU/Linux	**hardware architecture:**	amd64/x86

Description

While I'm importing several hundreds of images, I hit this error. Note that the ASAN reports says that some memory is freed from GTK which is apparently called from another thread than the main one:

```
==143888==ERROR: AddressSanitizer: attempting double-free on 0x61a000883280 in thread T0:
    #0 0x7fbdbb51b09e in __interceptor_realloc (/usr/lib/gcc/x86_64-pc-linux-gnu/4.9.3/libasan.so.
1+0x6209e)
    #1 0x7fbdb0db252e (/usr/lib64/libpixman-1.so.0+0x6b52e)
    #2 0x7fbdb0db3dc0 in pixman_region32_union (/usr/lib64/libpixman-1.so.0+0x6cdc0)
    #3 0x7fbdb9289989 in cairo_region_union (/usr/lib64/libcairo.so.2+0x75989)
    #4 0x7fbdb9e2e06d (/usr/lib64/libgdk-3.so.0+0x4a06d)
    #5 0x7fbdb9e2e1c1 (/usr/lib64/libgdk-3.so.0+0x4a1c1)
    #6 0x7fbdba4b658b in gtk_widget_unmap (/usr/lib64/libgtk-3.so.0+0x41b58b)
    #7 0x7fbdb89e38f7 in g_closure_invoke (/usr/lib64/libgobject-2.0.so.0+0x118f7)
    #8 0x7fbdb89fb306 (/usr/lib64/libgobject-2.0.so.0+0x29306)
    #9 0x7fbdb8a04fc1 in g_signal_emit_valist (/usr/lib64/libgobject-2.0.so.0+0x32fc1)
    #10 0x7fbdb8a05232 in g_signal_emit (/usr/lib64/libgobject-2.0.so.0+0x33232)
    #11 0x7fbdba4c4dbd in gtk_widget_hide (/usr/lib64/libgtk-3.so.0+0x429dbd)
    #12 0x7fbd8db66248 in _lib_recentcollection_updated ../src/libs/recentcollect.c:293
    #13 0x7fbdb89e38f7 in g_closure_invoke (/usr/lib64/libgobject-2.0.so.0+0x118f7)
    #14 0x7fbdb89fb9ea (/usr/lib64/libgobject-2.0.so.0+0x299ea)
    #15 0x7fbdb8a03eb7 in g_signal_emitv (/usr/lib64/libgobject-2.0.so.0+0x31eb7)
==143888==AddressSanitizer: while reporting a bug found another one.Ignoring.
    #16 0x7fbdbad80b29 in _signal_raise ../src/control/signal.c:158
    #17 0x7fbdb86d4d64 in g_main_context_invoke_full (/usr/lib64/libglib-2.0.so.0+0x57d64)
    #18 0x7fbdbad8152d in dt_control_signal_raise ../src/control/signal.c:240
    #19 0x7fbdbac464e3 in _dt_collection_recount_callback_2 ../src/common/collection.c:1269
    #20 0x7fbdb89e38f7 in g_closure_invoke (/usr/lib64/libgobject-2.0.so.0+0x118f7)
    #21 0x7fbdb89fb9ea (/usr/lib64/libgobject-2.0.so.0+0x299ea)
    #22 0x7fbdb8a03eb7 in g_signal_emitv (/usr/lib64/libgobject-2.0.so.0+0x31eb7)
    #23 0x7fbdbad80b29 in _signal_raise ../src/control/signal.c:158
    #24 0x7fbdb86d34bd in g_main_context_dispatch (/usr/lib64/libglib-2.0.so.0+0x564bd)
    #25 0x7fbdb86d38a7 (/usr/lib64/libglib-2.0.so.0+0x568a7)
    #26 0x7fbdb86d3d61 in g_main_loop_run (/usr/lib64/libglib-2.0.so.0+0x56d61)
    #27 0x7fbdba325e3c in gtk_main (/usr/lib64/libgtk-3.so.0+0x28ae3c)
    #28 0x7fbdbaf10ade in dt_gui_gtk_run ../src/gui/gtk.c:963
RawSpeed:RED,RawSpeed:GREEN,RawSpeed:
RawSpeed:GREEN,RawSpeed:BLUE,RawSpeed:
RawSpeed:DCRAW filter:94949494
RawSpeed:RED,RawSpeed:GREEN,RawSpeed:RED,RawSpeed:GREEN,RawSpeed:RED,RawSpeed:GREEN,RawSpeed:RED,R
awSpeed:GREEN,RawSpeed:
RawSpeed:GREEN,RawSpeed:BLUE,RawSpeed:GREEN,RawSpeed:BLUE,RawSpeed:GREEN,RawSpeed:BLUE,RawSpeed:GR
EEN,RawSpeed:BLUE,RawSpeed:
RawSpeed:DCRAW filter:94949494
    #29 0x55d9d8fe2f14 in main ../src/main.c:25
    #30 0x7fbdb3563733 in __libc_start_main (/lib64/libc.so.6+0x20733)
    #31 0x55d9d8fe2d78 in _start (/opt/darktable-debug/bin/darktable+0xd78)
```

```
0x61a000883280 is located 0 bytes inside of 1232-byte region [0x61a000883280,0x61a000883750)
freed by thread T3 here:
    #0 0x7fbdbb51b09e in __interceptor_realloc (/usr/lib/gcc/x86_64-pc-linux-gnu/4.9.3/libasan.so.
1+0x6209e)
    #1 0x7fbdb0db252e (/usr/lib64/libpixman-1.so.0+0x6b52e)
    #2 0x7fbdb0db3dc0 in pixman_region32_union (/usr/lib64/libpixman-1.so.0+0x6cdc0)
    #3 0x7fbdb9289989 in cairo_region_union (/usr/lib64/libcairo.so.2+0x75989)
    #4 0x7fbdb9e2e06d (/usr/lib64/libgdk-3.so.0+0x4a06d)
    #5 0x7fbdba4b6852 in gtk_widget_queue_draw_area (/usr/lib64/libgtk-3.so.0+0x41b852)
    #6 0x7fbdba4c3d4d in gtk_widget_queue_draw (/usr/lib64/libgtk-3.so.0+0x428d4d)
    #7 0x7fbdba4c3eb7 in gtk_widget_queue_resize (/usr/lib64/libgtk-3.so.0+0x428eb7)
    #8 0x7fbdba30ab7e (/usr/lib64/libgtk-3.so.0+0x26fb7e)
    #9 0x7fbdba30bc24 in gtk_label_set_markup (/usr/lib64/libgtk-3.so.0+0x270c24)
    #10 0x7fbd7e8c5c24 in _lib_hinter_set_message ../src/libs/tools/hinter.c:92
    #11 0x7fbdbad64871 in dt_control_hinter_message ../src/control/control.c:769
    #12 0x7fbdbac45c61 in dt_collection_hint_message ../src/common/collection.c:1214
    #13 0x7fbdbac3f19d in dt_collection_update ../src/common/collection.c:204
    #14 0x7fbdbac45550 in dt_collection_update_query ../src/common/collection.c:1177
    #15 0x7fbdbad2ff4b in dt_tag_attach ../src/common/tags.c:197
    #16 0x7fbdbacc983f in dt_image_import ../src/common/image.c:946
    #17 0x7fbdbaca5ba4 in dt_film_import1 ../src/common/film.c:465
    #18 0x7fbdbad7d176 in dt_film_import1_run ../src/control/jobs/film_jobs.c:31
    #19 0x7fbdbad6c032 in dt_control_run_job ../src/control/jobs.c:295
    #20 0x7fbdbad6d335 in dt_control_work ../src/control/jobs.c:526
    #21 0x7fbdb67c260b (/lib64/libpthread.so.0+0x760b)

previously allocated by thread T0 here:
    #0 0x7fbdbb51ad9f in malloc (/usr/lib/gcc/x86_64-pc-linux-gnu/4.9.3/libasan.so.1+0x61d9f)
    #1 0x7fbdb0db0c1a (/usr/lib64/libpixman-1.so.0+0x69c1a)
    #2 0x7fbdb0db2382 (/usr/lib64/libpixman-1.so.0+0x6b382)
    #3 0x7fbdb0db3dc0 in pixman_region32_union (/usr/lib64/libpixman-1.so.0+0x6cdc0)
    #4 0x7fbdb9289989 in cairo_region_union (/usr/lib64/libcairo.so.2+0x75989)
    #5 0x7fbdb9e2e06d (/usr/lib64/libgdk-3.so.0+0x4a06d)
    #6 0x7fbdb9e2e1c1 (/usr/lib64/libgdk-3.so.0+0x4a1c1)
    #7 0x7fbdba4b658b in gtk_widget_unmap (/usr/lib64/libgtk-3.so.0+0x41b58b)
    #8 0x7fbdb89e38f7 in g_closure_invoke (/usr/lib64/libgobject-2.0.so.0+0x118f7)
    #9 0x7fbdb89fb306 (/usr/lib64/libgobject-2.0.so.0+0x29306)
    #10 0x7fbdb8a04fc1 in g_signal_emit_valist (/usr/lib64/libgobject-2.0.so.0+0x32fc1)
    #11 0x7fbdb8a05232 in g_signal_emit (/usr/lib64/libgobject-2.0.so.0+0x33232)
    #12 0x7fbdba4c4dbd in gtk_widget_hide (/usr/lib64/libgtk-3.so.0+0x429dbd)
    #13 0x7fbd8db66248 in _lib_recentcollection_updated ../src/libs/recentcollect.c:293
    #14 0x7fbdb89e38f7 in g_closure_invoke (/usr/lib64/libgobject-2.0.so.0+0x118f7)
    #15 0x7fbdb89fb9ea (/usr/lib64/libgobject-2.0.so.0+0x299ea)
    #16 0x7fbdb8a03eb7 in g_signal_emitv (/usr/lib64/libgobject-2.0.so.0+0x31eb7)
    #17 0x7fbdbad80b29 in _signal_raise ../src/control/signal.c:158
    #18 0x7fbdb86d4d64 in g_main_context_invoke_full (/usr/lib64/libglib-2.0.so.0+0x57d64)
    #19 0x7fbdbad8152d in dt_control_signal_raise ../src/control/signal.c:240
    #20 0x7fbdbac464e3 in _dt_collection_recount_callback_2 ../src/common/collection.c:1269
    #21 0x7fbdb89e38f7 in g_closure_invoke (/usr/lib64/libgobject-2.0.so.0+0x118f7)
    #22 0x7fbdb89fb9ea (/usr/lib64/libgobject-2.0.so.0+0x299ea)
    #23 0x7fbdb8a03eb7 in g_signal_emitv (/usr/lib64/libgobject-2.0.so.0+0x31eb7)
    #24 0x7fbdbad80b29 in _signal_raise ../src/control/signal.c:158
    #25 0x7fbdb86d34bd in g_main_context_dispatch (/usr/lib64/libglib-2.0.so.0+0x564bd)
    #26 0x7fbdb86d38a7 (/usr/lib64/libglib-2.0.so.0+0x568a7)
    #27 0x7fbdb86d3d61 in g_main_loop_run (/usr/lib64/libglib-2.0.so.0+0x56d61)
    #28 0x7fbdba325e3c in gtk_main (/usr/lib64/libgtk-3.so.0+0x28ae3c)
    #29 0x7fbdbaf10ade in dt_gui_gtk_run ../src/gui/gtk.c:963

Thread T3 created by T0 here:
    #0 0x7fbdbb4de7a2 in pthread_create (/usr/lib/gcc/x86_64-pc-linux-gnu/4.9.3/libasan.so.1+0x257
a2)
    #1 0x7fbdbad6d69f in dt_control_jobs_init ../src/control/jobs.c:553
    #2 0x7fbdbad5e6fe in dt_control_init ../src/control/control.c:119
    #3 0x7fbdbac67ff4 in dt_init ../src/common/darktable.c:931
    #4 0x55d9d8fe2ec6 in main ../src/main.c:24
    #5 0x7fbdb3563733 in __libc_start_main (/lib64/libc.so.6+0x20733)
    #6 0x55d9d8fe2d78 in _start (/opt/darktable-debug/bin/darktable+0xd78)
```

```
SUMMARY: AddressSanitizer: double-free ??:0 __interceptor_realloc
==143888==ABORTING
```

I'm on Gentoo, DT from git 0ae79c07257923457914f5e63e19355d7772c624, with these packages:

```
x11-libs/gtk+-3.18.7:3::gentoo  USE="X cups introspection vim-syntax (-aqua) -broadway -cloudprint
 -colord -debug -examples {-test} -wayland -xinerama"
x11-libs/cairo-1.14.2::gentoo  USE="X glib opengl svg (-aqua) -debug (-directfb) (-gles2) -static-
libs -valgrind -xcb -xlib-xcb"
x11-libs/pixman-0.32.8::gentoo  USE="(-altivec) (-iwmmxt) (-loongson2f) (-neon) -static-libs"
dev-libs/glib-2.46.2-r3:2::gentoo  USE="dbus mime static-libs xattr -debug (-fam) (-selinux) -syst
emtap {-test} -utils"
```

Associated revisions

Revision e2f00fa5 - 06/07/2016 07:50 PM - Roman Lebedev

dt_collection_hint_message(): use g_idle_add(). Refs #11047

There are probably more places like this.
The problem is, dt_collection_update() can be called
from worker threads (non-T0), and it calls
dt_collection_hint_message(), which in the end
accesses GTK stuff. From non-T0.

FIXME: maybe dt_collection_update() should itself
be called from T0 in the same manner?

Revision 9d723f5e - 06/07/2016 10:10 PM - Roman Lebedev

dt_collection_update_query(): use g_idle_add() wrapped. Refs #11047

Avoids heap-use-after-free on import.

I do not really understand why collection.c is the way it is,
but this seems right..

```
=================================================================
17782ERROR: AddressSanitizer: heap-use-after-free on address 0x610000045140 at pc 0x7fb99cf973fe bp 0x7ffc9d0f3f20 sp 0x7ffc9d0f36d0
READ of size 2 at 0x610000045140 thread T0
RawSpeed:Shift left:1
RawSpeed:Shift down:1
RawSpeed:GREEN,RawSpeed:BLUE,RawSpeed:GREEN,RawSpeed:BLUE,RawSpeed:GREEN,RawSpeed:BLUE,RawSpeed:GREEN,RawSpeed:B
LUE,RawSpeed:
RawSpeed:RED,RawSpeed:GREEN,RawSpeed:RED,RawSpeed:GREEN,RawSpeed:RED,RawSpeed:GREEN,RawSpeed:RED,RawSpeed:GREEN,
RawSpeed:
RawSpeed:DCRAW filter:49494949
0 0x7fb99cf973fd  (/usr/lib/x86_64-linux-gnu/libasan.so.3+0x8b3fd)
1 0x7fb99cf97bba in vprintf (/usr/lib/x86_64-linux-gnu/libasan.so.3+0x8bbba)
2 0x7fb99cf97c77 in printf (/usr/lib/x86_64-linux-gnu/libasan.so.3+0x8bc77)
3 0x7fb97cc595b9 in _update_collected_images /home/lebedevri/darktable/src/views/lighttable.c:313
4 0x7fb97cc58f7a in _view_lighttable_collection_listener_callback /home/lebedevri/darktable/src/views/lighttable.c:274
5 0x7fb99a793fa4 in g_closure_invoke (/usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0+0xffa4)
6 0x7fb99a7a5fc0  (/usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0+0x21fc0)
7 0x7fb99a7add40 in g_signal_emitv (/usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0+0x29d40)
8 0x7fb99c9fd23f in _signal_raise /home/lebedevri/darktable/src/control/signal.c:158
9 0x7fb99a4b6059 in g_main_context_dispatch (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4a059)
10 0x7fb99a4b63ff  (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4a3ff)
11 0x7fb99a4b6721 in g_main_loop_run (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4a721)
12 0x7fb99c03c7d4 in gtk_main (/usr/lib/x86_64-linux-gnu/libgtk-3.so.0+0x2207d4)
13 0x7fb99cb68af8 in dt_gui_gtk_run /home/lebedevri/darktable/src/gui/gtk.c:963
```

14 0x400d90 in main /home/lebedevri/darktable/src/main.c:25
15 0x7fb99480c5ef in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x205ef)
16 0x400c58 in _start (/usr/local/bin/darktable+0x400c58)

0x610000045140 is located 0 bytes inside of 190-byte region [0x610000045140,0x6100000451fe)
freed by thread T3 here:
0 0x7fb99cfcd9d0 in free (/usr/lib/x86_64-linux-gnu/libasan.so.3+0xc19d0)
1 0x7fb99c8d624f in _dt_collection_store /home/lebedevri/darktable/src/common/collection.c:415
2 0x7fb99c8d5336 in dt_collection_update /home/lebedevri/darktable/src/common/collection.c:193
3 0x7fb99c8daf92 in dt_collection_update_query /home/lebedevri/darktable/src/common/collection.c:1177
4 0x7fb99c9b4d25 in dt_tag_attach /home/lebedevri/darktable/src/common/tags.c:197
5 0x7fb99c955e7a in dt_image_import /home/lebedevri/darktable/src/common/image.c:946
6 0x7fb99c93516b in dt_film_import1 /home/lebedevri/darktable/src/common/film.c:465
7 0x7fb99c9fa42e in dt_film_import1_run /home/lebedevri/darktable/src/control/jobs/film_jobs.c:31
8 0x7fb99c9eb440 in dt_control_run_job /home/lebedevri/darktable/src/control/jobs.c:295
9 0x7fb99c9ec5b1 in dt_control_work /home/lebedevri/darktable/src/control/jobs.c:526
10 0x7fb99836b463 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x7463)

previously allocated by thread T3 here:
0 0x7fb99cfcdce8 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.3+0xc1ce8)
1 0x7fb99a4bb728 in g_malloc (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4f728)

Thread T3 created by T0 here:
0 0x7fb99cf3cf19 in pthread_create (/usr/lib/x86_64-linux-gnu/libasan.so.3+0x30f19)
1 0x7fb99c9ec8d8 in dt_control_jobs_init /home/lebedevri/darktable/src/control/jobs.c:553
2 0x7fb99c9df7d6 in dt_control_init /home/lebedevri/darktable/src/control/control.c:119
3 0x7fb99c8fa53e in dt_init /home/lebedevri/darktable/src/common/darktable.c:931
4 0x400d4c in main /home/lebedevri/darktable/src/main.c:24
5 0x7fb99480c5ef in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x205ef)

SUMMARY: AddressSanitizer: heap-use-after-free (/usr/lib/x86_64-linux-gnu/libasan.so.3+0x8b3fd)
Shadow bytes around the buggy address:
0x0c20800009d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c20800009e0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c20800009f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
0x0c2080000a00: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c2080000a10: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c2080000a20: fa fa fa fa fa fa fa[fd]fd fd fd fd fd fd fd
0x0c2080000a30: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c2080000a40: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c2080000a50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c2080000a60: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c2080000a70: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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
Heap right redzone: fb
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack partial redzone: f4
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
17782ABORTING

Revision 38e08b1e - 06/13/2016 01:33 PM - Tobias Ellinghaus

Revert "dt_collection_update_query(): use g_idle_add() wrapped. Refs #11047"

This reverts commit 9d723f5e31c5516971cfe246352c926955376c97.
This introduces a bug where dt shows random images on startup and
eventually loads the right collection. Something better has to be come
up with. :-(

Revision 8edbb3a0 - 06/27/2016 04:05 PM - Roman Lebedev

dt_collection_hint_message(): use g_idle_add(). Refs #11047

There are probably more places like this.
The problem is, dt_collection_update() can be called
from worker threads (non-T0), and it calls
dt_collection_hint_message(), which in the end
accesses GTK stuff. From non-T0.

FIXME: maybe dt_collection_update() should itself
be called from T0 in the same manner?

(cherry picked from commit e2f00fa5bc02c779070a2f6ff1b3ccb6882a4665)

History

#1 - 06/07/2016 07:35 PM - Roman Lebedev

- Priority changed from Low to Medium

- Assignee set to Roman Lebedev

#2 - 01/17/2018 06:19 PM - Roman Lebedev

- Assignee deleted (Roman Lebedev)