# darktable - Bug #11336

## Crash while drawing mask in exposure module

11/27/2016 10:56 AM - Robert Hutton

| | | | |
|---|---|---|---|
| **Status:** | Fixed | **Start date:** | 11/27/2016 |
| **Priority:** | Low | **Due date:** | |
| **Assignee:** | | **% Done:** | 100% |
| **Category:** | Darkroom | **Estimated time:** | 0.00 hour |
| **Target version:** | 2.4.0 | | |
| **Affected Version:** | 2.2.0rc1 | **bitness:** | 64-bit |
| **System:** | Ubuntu | **hardware architecture:** | amd64/x86 |

**Description**

While drawing a mask using the path tool, in the exposure module.

```
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
0x00007fbe0bd2408b in __waitpid (pid=pid@entry=32025, stat_loc=stat_loc@entry=0x0, options=options@entry=0) at ../sysdeps/unix/sysv/linux/waitpid.c:29
29	../sysdeps/unix/sysv/linux/waitpid.c: No such file or directory.
backtrace written to /tmp/darktable_bt_HX5ERY.txt
Segmentation fault (core dumped)
```

### Associated revisions

**Revision 9e4f18dc - 11/29/2016 10:21 PM - Ulrich Pegelow**

drawn masks: reconsider use of dt_masks_free_form() towards a fix for bug #11336

**Revision 6e136c14 - 01/10/2017 10:43 AM - Ulrich Pegelow**

drawn masks: reconsider use of dt_masks_free_form() towards a fix for bug #11336

(cherry picked from commit 9e4f18dca27fd56984b34706e929dae1dece6959)

### History

**#1 - 11/27/2016 01:22 PM - Roman Lebedev**

Did you use new undo while working on this image?

**#2 - 11/27/2016 01:51 PM - Robert Hutton**

I don't think so; certainly not intentionally.

**#3 - 11/28/2016 09:25 PM - Ulrich Pegelow**

```
void dt_masks_free_form(dt_masks_form_t *form)
{
  if(!form) return;
  g_list_free_full(form->points, free);
  form->points = NULL;
  free(form);
  form = NULL;
  ^^^^^^^^^^^
}
```

That (^) doesn't look right. It only overwrites the argument in the called function, not (as it was supposedly intended) in the calling function. So we might get a double-free occasionally.

#### #4 - 11/28/2016 09:30 PM - Roman Lebedev

So far i was unable to reproduce this.
It might be related to #11276

#### #5 - 11/28/2016 09:37 PM - Ulrich Pegelow

> So far i was unable to reproduce this. It might be related to #11276

Sounds like a different thing to me. No masks mentioned. Do you agree that dt_masks_free_form() looks buggy? (I'm a bit slow today and want to make sure that I am not completely wrong). If yes we anyhow need to fix that thing. Will take care.

#### #6 - 11/28/2016 09:46 PM - Roman Lebedev

Ulrich Pegelow wrote:

> > So far i was unable to reproduce this. It might be related to #11276
>
> Sounds like a different thing to me. No masks mentioned.
>
> Do you agree that dt_masks_free_form() looks buggy? (I'm a bit slow today and want to make sure that I am not completely wrong). If yes we anyhow need to fix that thing. Will take care.

That

```
form = NULL;
```

does indeed look misplaced.

Something like this semantic patch should be a better fit

```
@@
expression e;
@@
<...
 dt_masks_free_form(e);
+ e = NULL;
...>
```

#### #7 - 11/28/2016 10:42 PM - Ulrich Pegelow

> Something like this semantic patch should be a better fit

Things might even be more complicated if one looks at path.c:dt_path_events_button_pressed() which is called by masks.c:dt_masks_events_button_pressed(). form is taken from darktable.develop->form_visible and potentially gets freed by using dt_masks_free_form(). Now all intermediate instances of form and the original storage place have to be set to NULL. This does not happen.

In order to fix we will need to use from by reference in any involved function calls which implies a lot of changes. IMHO that's too far reaching shortly before a release. I'm considering to only free form->points in dt_masks_free_form() and not free form itself, accepting the resulting memory leak.

#### #8 - 11/29/2016 08:36 AM - Roman Lebedev

Ulrich Pegelow wrote:

> > Something like this semantic patch should be a better fit
>
> Things might even be more complicated if one looks at path.c:dt_path_events_button_pressed() which is called by masks.c:dt_masks_events_button_pressed(). form is taken from darktable.develop->form_visible and potentially gets freed by using dt_masks_free_form(). Now all intermediate instances of form and the original storage place have to be set to NULL. This does not happen.
>
> In order to fix we will need to use from by reference in any involved function calls which implies a lot of changes. IMHO that's too far reaching shortly before a release.

All free() type functions take pointer that they should free, not ptr to pointer. Let's not invent wheel here at all, masks code is not nice as it is already :)

> I'm considering to only free form->points in dt_masks_free_form() and not free form itself,

And then the function will no longer match it's name. Maybe this should completely be left for after 2.2

> accepting the resulting memory leak.

uh

**#9 - 11/29/2016 08:42 AM - Ulrich Pegelow**

*- Status changed from New to Confirmed*

*- Target version changed from 2.2.0 to Future*

*- % Done changed from 0 to 10*

> Maybe this should completely be left for after 2.2

That's probably the best. So we leave fixing this bug for 2.3.

**#10 - 01/06/2017 10:34 AM - Ulrich Pegelow**

*- % Done changed from 10 to 100*

*- Status changed from Confirmed to Fixed*

Applied in changeset darktable|9e4f18dca27fd56984b34706e929dae1dece6959.

**#11 - 01/10/2017 09:22 PM - Roman Lebedev**

*- Target version changed from Future to 2.4.0*

## Files

| | | | |
|---|---|---|---|
| darktable_bt_HX5ERY.txt | 30.3 KB | 11/27/2016 | Robert Hutton |