Subject: TheIDE Format Setup BUG
Posted by Anonymous on Sat, 27 Nov 2010 10:53:24 GMT
View Forum Message <> Reply to Message

See attached video.

File Attachments
1) idebug.avi, downloaded 560 times

Subject: Re: TheIDE Format Setup BUG
Posted by dolik.rce on Sat, 27 Nov 2010 12:46:45 GMT
View Forum Message <> Reply to Message

Hi Andrei,

I think I encountered this bug. It is probably not related to theide, but to the ColorPusher. I encountered in other places as well, such as when setting a color of table borders in QTF editor. Strange is that I tried to reproduce this in Uword, but without any success. It happens at random, I can open it three or four times just fine and the fifth time it crashes (without even moving the cursor).

The crash itself is interesting too. It partially blocks my environment (XFCE on Arch Linux), I can't for example go to other desktops just by dragging mouse over the border of the screen (only keyboard shortcut works). The window stays on screen, with the dialog stopped in the middle of animation and only reacts to Alt+F4 (clicking the button on window border doesn't work, although it should be managed by WM as well, right?).

Honza

Subject: Re: TheIDE Format Setup BUG
Posted by koldo on Sat, 27 Nov 2010 13:17:08 GMT
View Forum Message <> Reply to Message

Hello

In windows XP it seems to work well.

Subject: Re: TheIDE Format Setup BUG
Posted by dolik.rce on Sat, 27 Nov 2010 16:08:13 GMT
View Forum Message <> Reply to Message

The bug is hidden in ImageX11.cpp, in function ImageDraw::operator Image(). At some point it asks X server for an image and the call fails returning NULL (at line 348). Later this NULL stored in pointer xim is accessed which inevitably leads to a crash.

Quick fix (i.e. removing the problem without really understanding what why the XGetImage fails):

```
ImageDraw::operator Image() const
{
 // ... a lot of code omitted here ...
 if(has_alpha) {
  xim = XGetImage(Xdisplay, alpha.dw, 0, 0, size.cx, size.cy, AllPlanes, ZPixmap);
  if(xim){    // added this check
   const byte *s = (const byte *)xim->data;
   t = ib;
   Buffer<RGBA> line(size.cx);
   for(int y = 0; y < size.cy; y++) {
    fmt.Read(line, s, size.cx, palette);
    for(int x = 0; x < size.cx; x++)
     (t++)->a = line[x].r;
    s += xim->bytes_per_line;
   }
   XDestroyImage(xim);
  }
 }
 Premultiply(ib);
 return ib;
}
```

As this fix bypasses the alpha processing (when the XGetImage fails), I would expect to see some visual artifacts, but I actually didn't notice anything. Maybe I was not looking hard enough or the effect is too subtle to see in the quick animation.

Also I have no idea why it makes problems in theide but I never seen it in any other app...

Best regards,
Honza

Subject: Re: TheIDE Format Setup BUG
Posted by mirek on Sat, 27 Nov 2010 17:15:03 GMT
View Forum Message <> Reply to Message

I think that as the first XGetImage:

```
 XImage *xim = XGetImage(Xdisplay, dw, 0, 0, max(size.cx, 1), max(size.cy, 1), AllPlanes,
ZPixmap);
```

specifically fixes zero size issue, the cause might be similar (zero sized image).

So, I am going to put this to "alpha" Image too, plus check for xim...

Subject: Re: TheIDE Format Setup BUG
Posted by dolik.rce on Sat, 27 Nov 2010 17:38:41 GMT
View Forum Message <> Reply to Message

Forget most of what I said in my previous post I dug deeper and found out that the reason why XGetImage fails is most probably that it is called on an image with one dimension equal to zero. The other calls are guarded against such thing, but this one for alpha layer was left unprotected.

I believe that if the image is empty (that is zero pixels in any direction, or in code GetSize().IsEmpty()==true), we don't have to bother drawing it at all, right? Or are there some side effects I didn't notice? I'd suggest something like: ImageDraw::operator Image() const
{
 if(size.IsEmpty()){ // this block is added
  ImageBuffer ib(size);
  return ib;
 }
 GuiLock __;
 XImage *xim = XGetImage(Xdisplay, dw, 0, 0, max(size.cx, 1), max(size.cy, 1), AllPlanes, ZPixmap);
 Visual *v = DefaultVisual(Xdisplay, Xscreenno);
 RasterFormat fmt;

 RGBA   palette[256];
// ...
}

For me it works fine and eliminates the crashes. The roll-out animation of color selector even looks a bit smoother now (but that might be just my imagination).

Oh, and I almost forgot to mention that the troublesome call to this operator Image() is located in Image WheelRampCtrl::PaintWheel(Size size) in DlgColor.cpp, in the "return iw;" statement (iw is the empty ImageDraw) where implicit conversion to Image happens.

Honza

Subject: Re: TheIDE Format Setup BUG
Posted by mirek on Sat, 04 Dec 2010 19:41:27 GMT
View Forum Message <> Reply to Message

dolik.rce wrote on Sat, 27 November 2010 12:38Forget most of what I said in my previous post I dug deeper and found out that the reason why XGetImage fails is most probably that it is called on an image with one dimension equal to zero. The other calls are guarded against such thing, but this one for alpha layer was left unprotected.

I believe that if the image is empty (that is zero pixels in any direction, or in code GetSize().IsEmpty()==true), we don't have to bother drawing it at all, right? Or are there some side effects I didn't notice? I'd suggest something like: ImageDraw::operator Image() const

```
{
 if(size.IsEmpty()){             // this block is added
  ImageBuffer ib(size);
  return ib;
 }
 GuiLock __;
 XImage *xim = XGetImage(Xdisplay, dw, 0, 0, max(size.cx, 1), max(size.cy, 1), AllPlanes,
ZPixmap);
 Visual *v = DefaultVisual(Xdisplay, Xscreenno);
 RasterFormat fmt;

 RGBA   palette[256];
// ...
}
```

For me it works fine and eliminates the crashes. The roll-out animation of color selector even looks a bit smoother now (but that might be just my imagination).

Oh, and I almost forgot to mention that the troublesome call to this operator Image() is located in Image WheelRampCtrl::PaintWheel(Size size) in DlgColor.cpp, in the "return iw;" statement (iw is the empty ImageDraw) where implicit conversion to Image happens.

Honza

I guess this is the (almost) same fix I am proposing in previous post - and which is in trunk already (well, since my previous post at least

Is current trunk working ok?

Mirek

Subject: Re: TheIDE Format Setup BUG
Posted by Anonymous on Sun, 05 Dec 2010 11:01:06 GMT
View Forum Message <> Reply to Message

mirek wrote on Sat, 04 December 2010 20:41
Is current trunk working ok?

Mirek

Yes, it seems ok.

Andrei

Subject: Re: TheIDE Format Setup BUG

Posted by sergeynikitin on Sun, 19 Jun 2011 11:07:20 GMT
View Forum Message <> Reply to Message

This bug came back to us! Help!

This patch does not work!

(environment: UBUNTU 10.10, U++ svn 3546)

Subject: Re: TheIDE Format Setup BUG
Posted by jibe on Tue, 21 Jun 2011 07:20:38 GMT
View Forum Message <> Reply to Message

Hi,

Pls see here, here and more especially here...

What is the opinion of the developpers ?

Subject: Re: TheIDE Format Setup BUG
Posted by sergeynikitin on Tue, 21 Jun 2011 18:24:43 GMT
View Forum Message <> Reply to Message

After this patch all went correct!

Subject: Re: TheIDE Format Setup BUG
Posted by jibe on Fri, 24 Jun 2011 07:12:09 GMT
View Forum Message <> Reply to Message

Hi,

sergeynikitin wrote on Tue, 21 June 2011 20:24After this patch all went correct!
Yes, good job ! Thanks for it

But in this post :
jibe wrote on Tue, 21 June 2011 09:10I think that the bug is deeper in the video code...

I should like to know the opinion of the developpers ?

The problems are still here in 3553 for lucid (last nightly build at this time). If your patch is really the right solution, why is it not included in the last version ?

This is a question to the developpers !

I can survive with this problem,
I can recompile with sergeynikitin's patches each time I download a new nightly build...
But if the problem can be definitely corrected, it would be better

---

Subject: Re: TheIDE Format Setup BUG
Posted by jibe on Mon, 27 Jun 2011 14:37:37 GMT
View Forum Message <> Reply to Message

Hi,

Is it possible to have some answer, opinion or advice from the developpers about these problems (including this one and this other that seem somehow similar), please ?

Even supposing that sergeynikitin's solution is not very good, at least it's useful ! If developpers have no time to solve this problem, or if they have difficulties because it's only with Linux (Ubuntu ?), at least could sergeynikitin's patches be added to the official release with a if statement, so that they are not used with windows ?
