Subject: BufferPainter Clip Crash - Fatal error: Invalid memory access!
Posted by devilsclaw on Wed, 25 Jan 2023 16:02:12 GMT
View Forum Message <> Reply to Message

So I found a combination of actions that will cause clipping to return a invalid pointer in RenderPath of BufferPainter.

1) Use Clip and Draw out side of the clip region
2) Attach the object to follow the mouse
3) Repeatedly move the mouse in and out of the window frame at the bottom in random locations up to 30 seconds.

Attached is an example app in code of how to cause it.

Below is the offending code and the output of it getting a corrupted pointer

Y2 is the pointer getting corrupted. Also I am on linux

```
if(clip.GetCount()) {
  printf("DC: Y1 = %i\n", y);
  const ClippingLine& s = clip.Top()[y];
  printf("DC: Y2 = %p\n", &s);
  if(s.IsEmpty()) {
    goto empty;
  }
  printf("DC: Y3 = %i\n", y);
  if(!s.IsFull()) {
    mf.Set(rg, s);
    rf = &mf;
  }
}
```

Results:
DC: Y1 = 525
DC: Y2 = 0x7f82b80571e8
DC: Y1 = 526
DC: Y2 = 0x7f82b80571f0
DC: Y3 = 526
DC: Y1 = 525
DC: Y2 = 0x7f82b80571e8
DC: Y1 = 526
DC: Y2 = 0x7f82b80571f0
DC: Y3 = 526
DC: MouseMove: x 16620 : y 16906 : 00000000
DC: Y1 = 526
DC: Y2 = 0x1070

File Attachments

1) DrawCrash.zip, downloaded 294 times