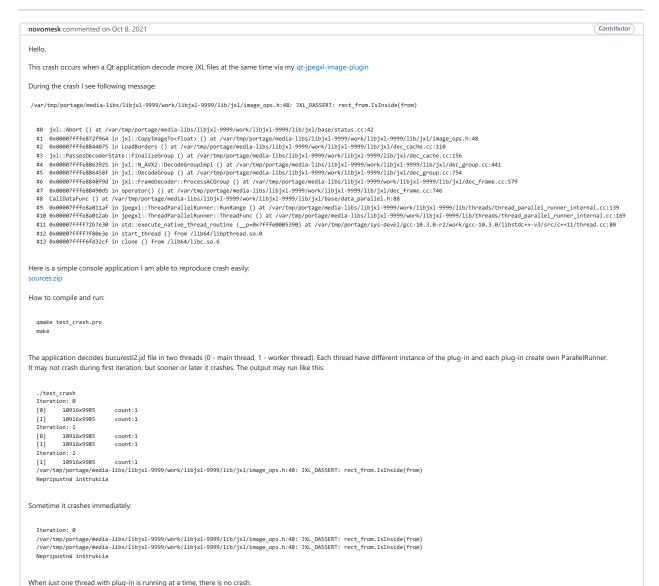
Jump to bottom New issue

Crash during multiple concurrent/parallel decoding #708



⊙ Closed) novomesk opened this issue on Oct 8, 2021 · 9 comments · Fixed by #775





povomesk mentioned this issue on Oct 8, 2021 error printed by jxlinfo #699

○ Closed

Contributor Author novomesk commented on Oct 8, 2021 If I put following call for <code>JXL_DEC_FULL_IMAGE</code> event into critical section, I can avoid crash: status = JxlDecoderProcessInput(m_decoder);

Contributor Author novomesk commented on Oct 9, 2021 I am able to reproduce the crash also via gdk-pixbuf loader which use ResizeableParallelRunner.

It is enough to call following procedure in concurrently in multiple threads few times:

```
#include <gdk-pixbuf/gdk-pixbuf.h>
bool test_plugin_gdk(int id)
{
    GdkPixbuf *pixbuf = gdk_pixbuf_new_from_file("bucuresti2.jx1", NULL);
    if (!pixbuf) {
        printf("Error reading picture via GDK plugin\n");
        return false;
    }
    int x = gdk_pixbuf_get_width(pixbuf);
    int y = gdk_pixbuf_get_height(pixbuf);
    printf("GDK [Xd]\tXdxXd\n", id, x, y);
    gdk_pixbuf_unref(pixbuf);
    return true;
}
```

saschanaz commented on Oct 11, 2021 • edited 🔻 djxl bucuresti2.jxl also fails, btw. ignion jonsneyers added bug decoder labels on Oct 13, 2021 A **@ deymo** self-assigned this on Oct 13, 2021 Contributor deymo commented on Oct 18, 2021 @novomesk what's the source image for that jxl file? Does it have a vertical green rectangle on the top right corner of the image by any chance? I'm not sure if that rectangle was on the source image or that's also a (maybe different) bug. I wasn't able to reproduce it directly with djxl but it has to do with the order in which the groups are processed so the more threads/CPUs you have the more likely it is. I was able to reliably reproduce it with an random-order single threaded parallel runner. novomesk commented on Oct 19, 2021 Contributor Author I think I found the source image here: https://www.skyscrapercity.com/threads/large-bucharest-photomap-10-000-x-10-000-pixels-38-mb-assembled-from-google-map-pieces.1673975/2000-pixels-38-mb-assemble-pixels-pixedeymo added a commit to deymo/libjxl that referenced this issue on Oct 26, 2021 Fix out of bounds copy in LoadBorders() ... 279a2e6 deymo mentioned this issue on Oct 26, 2021 Fix out of bounds copy in LoadBorders() #775 【 } • Merged) **C** deymo added a commit to deymo/libjxl that referenced this issue on Oct 26, 2021 732cf50 deymo added a commit to deymo/libjxl that referenced this issue on Oct 26, 2021 bb2b638 **G** deymo added a commit to deymo/libjxl that referenced this issue on Oct 26, 2021 Fix out of bounds copy in LoadBorders() ... e05e801 @ deymo closed this as completed in #775 on Oct 26, 2021 deymo added a commit that referenced this issue on Oct 26, 2021 Fix out of bounds copy in LoadBorders() (#775) ... ✓ e649705 deymo added a commit to deymo/libjxl that referenced this issue on Oct 27, 2021 Fix out of bounds copy in LoadBorders() (libjxl#775) ... X 435f2ac deymo commented on Oct 27, 2021 Contributor Thanks @novomesk for the link. The green rectangle is in the source image too, so that's good.

deymo commented on Oct 29, 2021

Note: this bug got assigned CVE-2021-22564

1 1

