
Subject: Crash when loading some jpeg files
Posted by [pvictor](#) on Tue, 10 Jan 2023 08:52:20 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi,

While working with thousands of jpeg files, I've found a few, which cause app crash.
One of them is attached.

Here's a simple testcase:

Test.upp:

```
description "Test\377";
```

```
uses
```

```
Core,  
plugin/jpg;
```

```
file
```

```
Test.cpp;
```

```
mainconfig
```

```
"" = "";
```

Test.cpp:

```
#include <Core/Core.h>  
#include <Draw/Draw.h>
```

```
using namespace Upp;
```

```
CONSOLE_APP_MAIN {  
    String im = LoadFile("/tmp/test.jpg");  
    Image img = StreamRaster::LoadStringAny(im); // Segmentation fault (core dumped)  
    Cout() << "OK\n";  
}
```

TheIDE: 16666

OS: Ubuntu 20.04

Best regards,

Victor

File Attachments

1) [test.jpg](#), downloaded 160 times

Subject: Re: Crash when loading some jpeg files
Posted by [pvictor](#) on Mon, 16 Jan 2023 09:09:53 GMT
[View Forum Message](#) <> [Reply to Message](#)

Well, after waiting for a while, I decided to find this bug myself.
I don't know if it is 100% correct, but it prevents crash on those unhappy images:
uppsrc/plugin/jpg/jpgupp.cpp: 384

```
- for(int diroff = Exif32(p + 4, end); diroff && begin + diroff < end; diroff = ExifDir(begin, end, diroff, BASE_IFD))  
+ for(int diroff = Exif32(p + 4, end); diroff>0 && begin + diroff < end; diroff = ExifDir(begin, end, diroff, BASE_IFD))
```

Best regards,
Victor
