# Exiv2 - Bug #534

## Integer overflow when reading thumbnail

14 Dec 2007 08:55 - Andreas Huggel

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Andreas Huggel | **% Done:** | 0% |
| **Category:** | exif | **Estimated time:** | 0.00 hour |
| **Target version:** | 0.16 | | |

**Description**

Mail from "Meder Kydyraliev" <meder@google.com>, 14-Dec-07:
---

Test: [fuzz-118.jpg] IFD1's (thumbnail IFD) JpegIFOffset(0x0201) and
JpegIFByteCount(0x0202) are set to values that overflow if added

exiv2-0.16-pre1:

- Test leads to an integer overflow in JpegThumbnail::setDataArea():

```
exif.cpp:

...
    308     if (len < offset + size) return 2;
    309     format->setDataArea(buf + offset, size);
    ...

value.hpp:

1600     template&lt;typename T&gt;
    1601     inline int ValueType&lt;T&gt;::setDataArea(const byte* buf, long len)
    1602     {
    1603         byte* tmp = 0;
    1604         if (len > 0) {
    1605             tmp = new byte[len];
    1606             std::memcpy(tmp, buf, len);
    1607         }

It seems like TiffThumbnail::setDataArea() might also have this problem.
```

Please credit "Meder Kydyraliev, Google Security Team" in any advisories
relating to these issues.

### History

**#1 - 14 Dec 2007 09:04 - Andreas Huggel**

r1345

(r1344 is not related to this issue, the svn comment is wrong.)

### Files

| | | | |
|---|---|---|---|
| fuzz-118.jpg | 43.5 KB | 14 Dec 2007 | Redmine Admin |