Exiv2 - Bug #886

Access violation on IptcData::operator[] when key is invalid

04 Mar 2013 10:17 - Robin Mills

Status:	Closed	**Start date:**	04 Mar 2013
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	iptc	**Estimated time:**	0.00 hour
Target version:	0.25		

Description

Christian has been kind enough to let me know about the following:

Using an invalid key, that exiv2 does not know, this function leads to an access violation.

```
Iptcdatum& IptcData::operator[](const std::string& key)
{
    IptcKey iptcKey(key);
    iterator pos = findKey(iptcKey);
    if (pos == end()) {
        add(Iptcdatum(iptcKey));
        pos = findKey(iptcKey);
    }
    return *pos;
}
```

Thanks, Christian. I'm not certain that this is a bug. I think the software has to throw an exception as he has no other way of saying "not found". Maybe you have to defend your calling code by using findKey(), or catching the exception.

History

#1 - 04 Mar 2013 11:55 - Christian Klinger

Maybe it's better to return a pointer than e reference. The pointer could be checked on NULL;
Yet the NULL pointer pos is dereferencd, which is not good. Another way is to check the pos, if it is NULL, then
to return an empty Iptcdatum.

But first once, I think I will use the findkey ()
To solve this problem is not urgent.

#2 - 04 Mar 2013 12:06 - Robin Mills

Christian. I'll investigate this after work this evening. I want to:

1. Be sure that findKey() is safe and does not crash.
2. Look at changing the API to return a ptr, however I think that'll ripple through the Exiv2 code and disturb client code.
3. Find out if we ever take the if (pos == end()) branch. Maybe that's a possible source of pain.

However I will investigate and update this report.

#3 - 04 Mar 2013 13:01 - Christian Klinger

Robin, thanks. But it is really not urgent. You should also enjoy your evenenig
after hard work.

#4 - 24 Jul 2013 15:52 - Robin Mills

- Target version changed from 0.24 to 0.25

Deferred to 0.25.

#5 - 07 Oct 2014 20:52 - Robin Mills

- Status changed from Assigned to Resolved

I'm going to mark this as resolved. Christian has a good idea that changing the API to returning a ptr (instead of reference) would enable the client test for NULL. However this involves changing the API which is very undesirable as it would disturb existing applications compiled against the existing API. There are two workarounds: 1) use an exception handler or 2) use findKey() before calling =.

#6 - 08 May 2015 16:23 - Robin Mills

- % Done changed from 0 to 100

#7 - 21 Jun 2015 16:42 - Andreas Huggel

- Status changed from Resolved to Closed