Exiv2 - Bug #1104

Buffer overflow in Exiv2::RiffVideo::dateTimeOriginal

10 Aug 2015 12:39 - Jakub Wilk

Status:	Assigned	**Start date:**	10 Aug 2015
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	10%
Category:	video	**Estimated time:**	30.00 hours
Target version:	1.0		

Description

Tested with svn r3885:

```
$ exiv2 pr crash.riff
*** Error in `exiv2': malloc(): memory corruption: 0x0000000000ed6aa0 ***
Aborted
```

Valgrind says it's a buffer overflow in Exiv2::RiffVideo::dateTimeOriginal:

```
==25760== Invalid write of size 8
==25760==    at 0x5DE490B: __GI_mempcpy (memcpy.S:272)
==25760==    by 0x5DD373D: _IO_file_xsgetn (fileops.c:1388)
==25760==    by 0x5DC954E: fread (iofread.c:42)
==25760==    by 0x51E4707: Exiv2::RiffVideo::dateTimeOriginal(long, int) (in /usr/local/lib/libexi
v2.so.14.0.0)
==25760==    by 0x51EA894: Exiv2::RiffVideo::decodeBlock() (in /usr/local/lib/libexiv2.so.14.0.0)
==25760==    by 0x51EAC27: Exiv2::RiffVideo::readMetadata() (in /usr/local/lib/libexiv2.so.14.0.0)
==25760==    by 0x41A87C: Action::Print::printSummary() (in /usr/local/bin/exiv2)
==25760==    by 0x41D4C7: Action::Print::run(std::string const&) (in /usr/local/bin/exiv2)
==25760==    by 0x405D5D: main (in /usr/local/bin/exiv2)
```

This bug was found using American fuzzy lop:
http://lcamtuf.coredump.cx/afl/

Related issues:

Related to Exiv2 - Feature #1028: Add GSoC13 video-write code	**Closed**	**01 Feb 2015**
Related to Exiv2 - Bug #1068: Video Code Umbrella	**Closed**	**26 Apr 2015**

History

#1 - 10 Aug 2015 12:45 - Jakub Wilk

In https://bugs.debian.org/781123#8, Vasyl Kaigorodov wrote:

> Just my 2c here - quickly looking at Valgrind backtrace, and the code -
> looks like the issue is that with attached crafted .riff file RiffVideo::tagDecoder() gets "unsigned long" as
> its' 2nd argument, which is then passed further to RiffVideo::dateTimeOriginal() as "long".
> I'm not a CPP guru, but other functions there might suffer from the same issue:
>
> junkHandler
> aviHeaderTagsHandler
> streamHandler
> streamDataTagHandler

#2 - 10 Aug 2015 12:47 - Jakub Wilk

- File crash.riff added

Of course I forgot the attachment. :)

#3 - 10 Aug 2015 22:03 - Thomas Beutlich

To answer your question on from https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=781123 : video support of exiv2 v0.25 was not accidentally disabled but by purpose for the very reason of bugs like this one.

#4 - 21 Aug 2015 17:03 - Robin Mills

- Category set to video

- Status changed from New to Assigned

- Assignee set to Robin Mills

- Target version set to 0.26

#5 - 24 Sep 2015 11:12 - Robin Mills

- % Done changed from 0 to 10

- Estimated time set to 30.00 h

I suspect there is rather a lot of effort required here to test for buffer overflows in the video code.

#6 - 27 Mar 2016 09:32 - Robin Mills

- Target version changed from 0.26 to 1.0

This is being deferred for v0.26. I hope refactoring the video code will be the headline feature of v0.27.

Files

crash.riff	1.11 KB	10 Aug 2015	Jakub Wilk