Exiv2 - Bug #890

ASF: heap overflow

11 Mar 2013 07:49 - Alyssa Milburn

Status:	Closed	**Start date:**	11 Mar 2013
Priority:	Normal	**Due date:**	
Assignee:	Abhinav Badola	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	0.24		

Description

asfvideo.cpp:624 reads dataLength amount of data into a buffer of size 500, causing a heap overflow if dataLength>500. Testcase attached.

At a glance lines 617, 630, 638 probably also have similar problems. Also quicktimevideo.cpp:1059/1066/1077/1095?

Associated revisions

Revision 2996 - 13 Mar 2013 13:52 - Abhinav Badola

#890: Corrected the case of Infinite loop in RiffVideo::nikonTagsHandler()

Revision 2997 - 13 Mar 2013 14:45 - Abhinav Badola

#890: Corrected the case of heap overflow if dataLength>500 in asfvideo.cpp, quicktimevideo.cpp

Revision 2999 - 26 Mar 2013 01:36 - Abhinav Badola

#890: Fixed some possible issues of crashing due to in-efficient management of buffers in riffvideo.cpp

Revision 3000 - 26 Mar 2013 02:14 - Abhinav Badola

#890: Fixed some possible issues of crashing due to in-efficient management of buffers in asfvideo.cpp

Revision 3001 - 26 Mar 2013 14:11 - Abhinav Badola

#890: Fixed some possible issues of crashing due to underflow in buffers in quicktimevideo.cpp

History

#1 - 11 Mar 2013 08:22 - Abhinav Badola

- Assignee set to Abhinav Badola

#2 - 13 Mar 2013 14:56 - Abhinav Badola

- % Done changed from 0 to 50

Hi Alyssa,

Please test and confirm if this bug is also solved at your end.

Thanking you in anticipation.

#3 - 13 Mar 2013 15:35 - Alyssa Milburn

That certainly fixes my testcase. I'll check the other cases, thanks for the quick response.

Unfortunately (sorry!) I didn't look carefully enough the first time. Here's some more possible issues:

asfvideo.cpp:560/570/580, riffvideo.cpp:764/786/856 might have the same problem. riffvideo.cpp:654 also looks unsafe (the size comes from line 572?).

riffvideo.cpp:927 might be unsafe in 32-bit builds because the allocation on riffvideo.cpp:868 looks like it can be overflowed (if I provide a size of -1).

Obviously I'm not very familiar with the exiv2 code, but a lot of the other code uses a separate buffer and passes that buf.size_ to the io_->read calls, so there's no chance of a heap overflow. Perhaps it might be worth doing that in some of these cases.

#4 - 13 Mar 2013 16:16 - Alyssa Milburn

- File overflow2.mov added

You need to also check for dataLength being too low in your new checks on quicktimevideo.cpp:1082/1100/1119/1138, because you subtract a constant from it during the actual read(). Another (manually constructed) testcase attached.

#5 - 14 Mar 2013 05:41 - Abhinav Badola

Alyssa Milburn wrote:

> That certainly fixes my testcase. I'll check the other cases, thanks for the quick response.
>
> Unfortunately (sorry!) I didn't look carefully enough the first time. Here's some more possible issues:

Don't worry. We are happy to have you here, reporting these issues.
Lets keep this issue open till all the bugs are solved.

It is better that we take some more time on analyzing and fixing bugs right now, than having major program crashes later.
Thank you for analyzing Exiv2, and helping in making it more sturdy and robust.

I will keep on patching the issues that you may find, meanwhile I will expect you to find more.

#6 - 14 Mar 2013 10:30 - Robin Mills

I'd like to thank both of you for working on this stuff. Fuzzing and hardening the code is good for everybody. Thank you both for working on this.

A couple of questions for Alyssa:
1) Would it help you if we grant you write access to the depot?
2) There's a corrupted file being discussed in Forum topic 1477
http://dev.exiv2.org/boards/3/topics/1477

I'm going to take a look at Aleksandr's file this evening. If you have time and interest to investigate, I would very much appreciate your analysis.

Robin

#7 - 14 Mar 2013 15:06 - Alyssa Milburn

If Abhinav or others familiar with the project can find the time to fix these bugs, then I think it's a much better idea for them to make the fixes, since they're in a much better position to test the code (and are presumably going to be maintaining it in the long-term). If you need suggested patches for any of these issues then I can make an attempt, though.

Beware that I'm not running an actual fuzzer, and there might well be other obvious bugs which would be caught by one; my filed bugs are just the result of my glancing through the source code and seeing if I spot any suspicious-looking code.

(The file in the forum post seems to be corrupt/truncated as diagnosed; I don't think I can add anything to what's already been said.)

#8 - 14 Mar 2013 15:09 - Robin Mills

- Status changed from New to Assigned

Thanks for updating us, Alyssa. I'm glad you have the time to just "glance through the code". You're spotting good things. I haven't looked at that corrupted file in Topic 1477, however I'll have a look at it this evening.

#9 - 26 Mar 2013 14:16 - Abhinav Badola

Hi Alyssa,
I have submitted some new commits. Please ensure that the bugs that you noticed before have been taken care off.
If you think there are some more vulnerable issues, then please inform us whenever you get time.

Else I would like to close both the issue #890 and #888.

#10 - 05 May 2013 04:45 - Abhinav Badola

- Status changed from Assigned to Resolved

- % Done changed from 50 to 100

#11 - 24 Jul 2013 15:08 - Robin Mills

- Status changed from Resolved to Closed

- Target version set to 0.24

Fixed in 0.24.

Files

heap-overflow.asf	64.1 KB	11 Mar 2013	Alyssa Milburn
overflow2.mov	288 Bytes	13 Mar 2013	Alyssa Milburn