Exiv2 - Bug #891

MRW: potential infinite loop on invalid input

12 Mar 2013 13:32 - Alyssa Milburn

Status:	New	**Start date:**	12 Mar 2013
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	exif	**Estimated time:**	0.00 hour
Target version:	0.28		

Description

In 32-bit builds, the seek on mrwimage.cpp:135 can be backwards if the input file has a large enough value for siz, and since mrwimage.cpp:133 also overflows, this can lead to an infinite loop if you set siz=-len. Testcase attached.

History

#1 - 15 Mar 2013 15:35 - Robin Mills

- Category set to exif

- Status changed from New to Assigned

- Assignee set to Robin Mills

- Priority changed from Low to Normal

- Target version set to 0.24

Thanks, Alyssa. I'll take a look at this.

#2 - 24 Jul 2013 15:52 - Robin Mills

- Target version changed from 0.24 to 0.25

Deferred to 0.25.

#3 - 09 May 2015 08:23 - Robin Mills

- Target version changed from 0.25 to 0.26

Deferred to v0.26. Insufficient time to deal with this for v0.25.

#4 - 23 May 2015 08:44 - Robin Mills

- Assignee deleted (Robin Mills)

#5 - 16 Sep 2016 06:55 - Robin Mills

- Status changed from Assigned to New

- Target version changed from 0.26 to 0.28

I've put in around 1200 hours of unpaid work to get to code complete v0.26 and closed almost 200 issues. Regrettably, there are only 5 or 6 issues on which I have not been able to work. This is one. Deferred for v0.27.

Files

infinite-loop.mrw	16 Bytes	12 Mar 2013	Alyssa Milburn