CrystaX NDK - Bug #1369

SIGSEGV in libcrystax.so - lrintf

04/21/2016 06:48 PM - Jakob Raible

Status:	Closed	**Start date:**	04/21/2016
Priority:	High	**Due date:**	
Assignee:	Dmitry Moskalchuk	**% Done:**	100%
Category:	libcrystax	**Estimated time:**	0.00 hour
Target version:	11.0.0		
CPU Architecture:	arm	**Android version:**	4.1 (android-16)
Host OS:	OS X	**CrystaX Version:**	10.3.1
Toolchain:			

Description

Hi,
my Android gradle project builds fine and starts to run on my Android device, however I always get a SIGSEGV at a certain line.
This project is a multi-platform project and all the other platforms (OS X, iOS) work fine. It also worked with Google's NDK r10d.
I'm also using OpenCV 3.1 and compiled it successfully with your cmake toolchain with the newest daily build.
I'm building for armeabi-v7a.
Is this a bug in Crystax or am I doing something wrong here?

I get the following stack trace:

```
04-21 17:33:23.909    4775-4858/de.formigas.lottoscanner A/libc Fatal signal 11 (SIGSEGV), code 2, fault addr 0x9d536ffc in tid
4858 (AsyncTask #2)
04-21 17:33:24.011      191-191/? A/DEBUG *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
04-21 17:33:24.011      191-191/? A/DEBUG Build fingerprint: 'google/razor/flo:6.0.1/MMB29K/2419427:user/release-keys'
04-21 17:33:24.011      191-191/? A/DEBUG Revision: '0'
04-21 17:33:24.011      191-191/? A/DEBUG ABI: 'arm'
04-21 17:33:24.011      191-191/? A/DEBUG pid: 4775, tid: 4858, name: AsyncTask #2  >>> de.formigas.lottoscanner <<<
04-21 17:33:24.011      191-191/? A/DEBUG signal 11 (SIGSEGV), code 2 (SEGV_ACCERR), fault addr 0x9d536ffc
04-21 17:33:24.036      191-191/? A/DEBUG r0 9d53700c  r1 00000001  r2 88000000  r3 88000000
04-21 17:33:24.036      191-191/? A/DEBUG r4 9d53700c  r5 43aa0000  r6 9d637f88  r7 02010000
04-21 17:33:24.036      191-191/? A/DEBUG r8 00000020  r9 b4d4abf4  sl cccccccd  fp 00000000
04-21 17:33:24.036      191-191/? A/DEBUG ip b37b7cb8  sp 9d537008  lr b37a5b8f  pc b3768c9c  cpsr 60070030
04-21 17:33:24.038      191-191/? A/DEBUG backtrace:
04-21 17:33:24.039      191-191/? A/DEBUG #00 pc 0001dc9c  /data/app/de.formigas.lottoscanner-1/lib/arm/libcrystax.so
04-21 17:33:24.039      191-191/? A/DEBUG #01 pc 0005ab8b  /data/app/de.formigas.lottoscanner-1/lib/arm/libcrystax.so (lrintf+10)
```

Related issues:

Is duplicate of CrystaX NDK - Bug #1380: SIGSEGV in libcrystax.so - lrint	**Duplicated**	**04/29/2016**

History

#1 - 04/21/2016 06:51 PM - Dmitry Moskalchuk

- Category set to libcrystax

- Assignee set to Dmitry Moskalchuk

- Priority changed from Normal to High

Jakob Raible wrote:

> Is this a bug in Crystax or am I doing something wrong here?

Well, if it crashes, it looks as a bug. Could you provide some minimal example to reproduce the problem? I could say more detailed then what's wrong.

#2 - 04/22/2016 01:34 PM - Jakob Raible

Dmitry Moskalchuk wrote:

> Jakob Raible wrote:
>
> > Is this a bug in Crystax or am I doing something wrong here?
>
> Well, if it crashes, it looks as a bug. Could you provide some minimal example to reproduce the problem? I could say more detailed then what's wrong.

Thanks for the quick reply!
I digged a little deeper and it definitely has to do with some implicit float to int casting. lrintf seems to be causing the error somehow, as the stack trace already suggests.
An example which leads to a crash is the following:

cv::Point2f pf = cv::Point2f(1.0, 2.0);
cv::Point p = pf;

I'm still busy creating a minimal example, but this might already help you!
Thanks for your efforts!

#3 - 04/22/2016 02:20 PM - Dmitry Moskalchuk

Jakob Raible wrote:

> I'm still busy creating a minimal example, but this might already help you!

OK, I confirm that lrintf cause the crash on minimal example:

```
#include <math.h>
#include <stdio.h>

int main()
{
    long v = lrintf(23.45f);
    printf("v=%ld\n", v);
    return 0;
}
```

Call stack points inside fegetenv, which is implicitly called from lrintf. It's unclear yet why this happens, but I'm going to figure out what's wrong and fix it.

Thank you for reporting it!

#4 - 05/04/2016 07:48 PM - Dmitry Moskalchuk

- Is duplicate of Bug #1380: SIGSEGV in libcrystax.so - lrint added

#5 - 05/04/2016 07:50 PM - Dmitry Moskalchuk

- Status changed from Open to Duplicated

- % Done changed from 0 to 100

This is actually the same bug as #1369 – i.e. crash is caused by call of fegetenv – so close it as "duplicate".

#6 - 05/05/2016 01:23 PM - Dmitry Moskalchuk

- Status changed from Duplicated to Open

- % Done changed from 100 to 0

Here is test case

#7 - 05/20/2016 06:21 PM - Dmitry Moskalchuk

- Status changed from Open to Closed

- % Done changed from 0 to 100

Fixed

Will be included to the NDK build #854 (https://dl.crystax.net/builds/)