CrystaX NDK - Bug #1442

SIGSEGV in libCoreFoundation

07/14/2016 06:25 PM - Andrew Druk

Status:	Open	**Start date:**	07/14/2016
Priority:	High	**Due date:**	
Assignee:	Dmitry Moskalchuk	**% Done:**	0%
Category:	cocotron	**Estimated time:**	0.00 hour
Target version:	11.0.0		
CPU Architecture:	x86, x86_64	**Android version:**	5.0 (android-21), 6.0 (android-23)
Host OS:	OS X	**CrystaX Version:**	10.3.1
Toolchain:	clang-3.7		

Description

```
#import <stdio.h>
#import <Foundation/Foundation.h>

int main()
{
    NSThread* _thread = [NSThread new];
    [_thread start];
    sleep(2);
    return 0;
}

Fatal signal 11 (SIGSEGV), code 1, fault addr 0x0 in tid 9146 (ddle.objcsample)[ 07-14 18:13:48.81
2  1216: 1216 W/debuggerd: handling request: pid=9130 uid=10065 gid=10065 tid=9146
 *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
 Build fingerprint: 'Android/sdk_google_phone_x86_64/generic_x86_64:N/NPD56O/2964822:userdebug/tes
t-keys'
 Revision: '0'
 ABI: 'x86_64'
 pid: 9130, tid: 9146, name: ddle.objcsample  >>> com.readdle.objcsample <<<
 signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x0
     rax 0000000000000000  rbx 00007ffeec836000  rcx 00007ffedbbff450  rdx 0000000000000001
     rsi 00007ffedc0d5690  rdi 0000000000000270
     r8  0000000000000080  r9  00007ffedbbfe940  r10 00007ffedc034e10  r11 000000000000011d
     r12 00007ffedbbff450  r13 00007ffedc0978a0  r14 00007ffedbbff450  r15 00007ffedbbff4e8
     cs  0000000000000033  ss  000000000000002b
     rip 00007ffedc0d51a8  rbp 00007ffedbbff390  rsp 00007ffedbbff360  eflags 0000000000000246
 backtrace:
     #00 pc 000000000029d1a8  /data/app/com.readdle.objcsample-2/lib/x86_64/libCoreFoundation.so (
objc_autoreleasePoolPush+24)
     #01 pc 00000000001fce24  /data/app/com.readdle.objcsample-2/lib/x86_64/libCoreFoundation.so (
_i_NSAutoreleasePool__init+20)
     #02 pc 000000000025f934  /data/app/com.readdle.objcsample-2/lib/x86_64/libCoreFoundation.so (
nsThreadStartThread+148)
     #03 pc 0000000000089731  /system/lib64/libc.so (_ZL15__pthread_startPv+177)
     #04 pc 00000000000299eb  /system/lib64/libc.so (__start_thread+11)
     #05 pc 000000000001ca65  /system/lib64/libc.so (__bionic_clone+53)
```

History

#1 - 07/14/2016 06:35 PM - Dmitry Moskalchuk

- Category set to cocotron

- Assignee set to Dmitry Moskalchuk

- Priority changed from Normal to High

#2 - 07/14/2016 06:37 PM - Dmitry Moskalchuk

Thank you for report!

BTW, how exactly you build it? Could you please provide exact copy of all command line commands with its parameters causing such crash?

#3 - 07/14/2016 06:40 PM - Dmitry Moskalchuk

- Description updated

#4 - 07/15/2016 04:27 PM - Andrew Druk

I built it with just 'ndk-build'

Application.mk

```
APP_ABI := all
NDK_TOOLCHAIN_VERSION := clang3.7
APP_OBJC := cocotron
```

Android.mk

```
LOCAL_PATH := $(call my-dir)

include $(CLEAR_VARS)
LOCAL_MODULE     := test
LOCAL_SRC_FILES  := test.m
include $(BUILD_EXECUTABLE)
```

Then I pushed all .so and executable to emulator's /data/local/tmp and I executed it with appropriate LD_LIBRARY_PATH.