CrystaX NDK - Bug #958

use [popen] get stream handle,and [fread]or[fgets] crash

05/29/2015 06:17 PM - Beily Lan

Status:	Closed	**Start date:**	05/29/2015
Priority:	Urgent	**Due date:**	
Assignee:	Dmitry Moskalchuk	**% Done:**	100%
Category:	libcrystax	**Estimated time:**	0.00 hour
Target version:	10.2.0		
CPU Architecture:	arm	**Android version:**	4.3 (android-18)
Host OS:	Windows	**CrystaX Version:**	
Toolchain:	gcc-4.9		

Description

when use *crystax-ndk-10.1.0 NDK* build OK, but *run Crash*, i get an error. by the way, in our website i cant find 10.2.0 or higher version to download.so i have no idea, if the higher verion has fix the bug.
error as follow:
05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute ,cmd = ls.
05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute ,popen success=====.
05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute, command=ls 2>&1
05-29 20:53:46.677: A/libc(19241): invalid address or address of corrupt block 0x40161c30 passed to dlfree [here "fread"or"fgets" execute]
05-29 20:53:46.687: A/libc(19241): Fatal signal 11 (SIGSEGV) at 0xdeadbaad (code=1), thread 19241 (xample.myapp002)

But, if use *google android-ndk-r10d NDK* , build *OK* and run *OK*, it work find, and i can get the result of execute [ls] command.
So, i think it maybe a crystax NDK's BUG. pls let me know, if your have good news,thank u very much! best wishes!

PS:
IDE : Eclipse
HostOS: Windows + cgywin64

History

#1 - 05/29/2015 08:58 PM - Alexander Zhukov

Beily Lan wrote:

> when use *crystax-ndk-10.1.0 NDK* build OK, but *run Crash*, i get an error. by the way, in our website i cant find 10.2.0 or higher version to download.so i have no idea, if the higher verion has fix the bug.
> error as follow:
> 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute ,cmd = ls.
> 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute ,popen success=====.
> 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute, command=ls 2>&1
> 05-29 20:53:46.677: A/libc(19241): invalid address or address of corrupt block 0x40161c30 passed to dlfree [here "fread"or"fgets" execute]
> 05-29 20:53:46.687: A/libc(19241): Fatal signal 11 (SIGSEGV) at 0xdeadbaad (code=1), thread 19241 (xample.myapp002)
>
> But, if use *google android-ndk-r10d NDK* , build *OK* and run *OK*, it work find, and i can get the result of execute [ls] command.
> So, i think it maybe a crystax NDK's BUG. pls let me know, if your have good news,thank u very much! best wishes!
>
> PS:
> IDE : Eclipse
> HostOS: Windows + cgywin64

Could you please provide a minimal source code required to reproduce the bug?

BTW 10.2.0 is planned, not released yet.

#2 - 06/01/2015 04:46 PM - Beily Lan

- File MyApp002-popen-fread-crash-002.txt added

Alexander Zhukov wrote:

> Beily Lan wrote:

> when use *crystax-ndk-10.1.0 NDK* build OK, but *run Crash*, i get an error. by the way, in our website i cant find 10.2.0 or higher version to download.so i have no idea, if the higher verion has fix the bug.
> error as follow:
> 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute ,cmd = ls.
> 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute ,popen success=====.
> 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute, command=ls 2>&1
> 05-29 20:53:46.677: A/libc(19241): invalid address or address of corrupt block 0x40161c30 passed to dlfree [here "fread"or"fgets" execute]
> 05-29 20:53:46.687: A/libc(19241): Fatal signal 11 (SIGSEGV) at 0xdeadbaad (code=1), thread 19241 (xample.myapp002)
>
> But, if use *google android-ndk-r10d NDK* , build *OK* and run *OK*, it work find, and i can get the result of execute [ls] command.
> So, i think it maybe a crystax NDK's BUG. pls let me know, if your have good news,thank u very much! best wishes!
>
> PS:
> IDE : Eclipse
> HostOS: Windows + cgywin64

Could you please provide a minimal source code required to reproduce the bug?

BTW 10.2.0 is planned, not released yet.

Of course! :)
Actually,last time i had attached my whole Eclipse project(java/c++ source Files), which like MyApp002.rar. maybe, upload fail
This i will upload again.

#3 - 06/01/2015 05:26 PM - Beily Lan

- File MyApp002-----.rar added

- File MyApp002.apk added

Beily Lan wrote:

> Alexander Zhukov wrote:
>
> > Beily Lan wrote:
> >
> > > when use *crystax-ndk-10.1.0 NDK* build OK, but *run Crash*, i get an error. by the way, in our website i cant find 10.2.0 or higher version to download.so i have no idea, if the higher verion has fix the bug.
> > > error as follow:
> > > 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute ,cmd = ls.
> > > 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute ,popen success=====.
> > > 05-29 20:53:36.677: I/MyAppTest002(19241): JNI::execute, command=ls 2>&1
> > > 05-29 20:53:46.677: A/libc(19241): invalid address or address of corrupt block 0x40161c30 passed to dlfree [here "fread"or"fgets" execute]
> > > 05-29 20:53:46.687: A/libc(19241): Fatal signal 11 (SIGSEGV) at 0xdeadbaad (code=1), thread 19241 (xample.myapp002)
> > >
> > > But, if use *google android-ndk-r10d NDK* , build *OK* and run *OK*, it work find, and i can get the result of execute [ls] command.
> > > So, i think it maybe a crystax NDK's BUG. pls let me know, if your have good news,thank u very much! best wishes!
> > >
> > > PS:
> > > IDE : Eclipse
> > > HostOS: Windows + cgywin64
> >
> > Could you please provide a minimal source code required to reproduce the bug?
> >
> > BTW 10.2.0 is planned, not released yet.
>
> Of course! :)
> Actually,last time i had attached my whole Eclipse project(java/c++ source Files), which like MyApp002.rar. maybe, upload fail
> This time i will upload again.
> as follow, the main file:
> [java]
> 1, MainActivity.java : this file is to listening UI button action;
> case R.id.MyButton:
> {
> textViewMsgShow.setText("This MyButton Click");
> String cmd = "ls 2>&1"; //command shell. ls
> String res = pCmd.exec(cmd); // here will call native exec function,if it execute OK , will return SUCCESS
> if(!res.isEmpty())
> {
> textViewMsgShow.setText(res); // here show the result string

}
break;
}
2,CmdCentre.java : this file like interface, for loading library and declaring native functions. here is only one .
static {
// //if use google NDK , we dont load crystax lib
System.loadLibrary("crystax");
System.loadLibrary("NDK1");
}

```
// JNI function, delare
public native String exec(String cmd);
```

==========
[C++/jni]
1, NDK1.cpp : this file impliment the native funtion "exec"

std::string exec(char* cmd) {

```
char result_buf[MAXLINE], command[MAXLINE];
int rc = 0; // command exec return
int totalReadSize = 0;
FILE *fp = 0;
fp = popen(cmd, "r");
if(NULL == fp)
{
    __android_log_print(ANDROID_LOG_INFO, LOG_TAG,"popen fail ");
    return "";
}

__android_log_print(ANDROID_LOG_INFO, LOG_TAG, "JNI::execute ,popen success=====.");
__android_log_print(ANDROID_LOG_INFO, LOG_TAG, "JNI::execute, command=%s",cmd);

sleep(10);

while(!feof(fp))
{
    int iReadSize = 0;
    __android_log_print(ANDROID_LOG_INFO, LOG_TAG, "Before fread");
    iReadSize = fread(result_buf, 1, 64, fp); //here Crash with cryStax NDK, OK for google NDK
    __android_log_print(ANDROID_LOG_INFO, LOG_TAG, "After fread");
    if('\n' == result_buf[strlen(result_buf)-1])
    {
        result_buf[strlen(result_buf)-1] = '\0';
    }

    __android_log_print(ANDROID_LOG_INFO, LOG_TAG,"command[%s] Out= [ %s ]", cmd, result_buf);
    totalReadSize += iReadSize;
}
__android_log_print(ANDROID_LOG_INFO, LOG_TAG,"totalReadSize=%d",totalReadSize);

rc = pclose(fp);
if(-1 == rc)
{
    __android_log_print(ANDROID_LOG_INFO, LOG_TAG,"close stream fail");
    return "";
}
else
{
    __android_log_print(ANDROID_LOG_INFO, LOG_TAG,"[%s] child process return=[%d], command return=[%d]\r\n", c
md, rc, WEXITSTATUS(rc));
}
```

return "SUCCESS";
}

extern "C" {

```
  jstring Java_com_example_myapp002_CmdCentre_exec(JNIEnv* env,
            jobject thiz,
            jstring cmd)
  {

    const char *res = env->GetStringUTFChars(cmd, NULL);
```

```
    __android_log_print(ANDROID_LOG_INFO, LOG_TAG, "JNI::execute ,cmd = %s.",res);

    std::string result = exec((char*)res);
    env->ReleaseStringUTFChars(cmd, res);
  return env->NewStringUTF(result.c_str());
 }
```

}

above is that three files main code. detail you can reference attachment MyApp002----.rar
Thank u, Alexander, Best wish!

#4 - 06/05/2015 02:50 PM - Dmitry Moskalchuk

- Assignee changed from Alexander Zhukov to Dmitry Moskalchuk

#5 - 06/11/2015 02:21 PM - Dmitry Moskalchuk

- Status changed from Open to Closed

- % Done changed from 0 to 100

"Fixed":https://github.com/crystax/android-platform-ndk/commit/2eecd0a03bd1ae8fdb0978d9bb5a288bb29492d7. Will be included to the next release.

#6 - 06/25/2015 06:52 AM - Beily Lan

Thank you tell me the good news.
And I have find other interesting thing,
also , i use "popen" to execute command and get the file handle return,
then, i convert the file handle to file discriptor by "fileno" function.
then, i can get the Result by "read" function.
In this way, its work well.
Is it interesting? but i dont know why.
If you have time, please give us more detials for this bug, with next release version.
think you all!

#7 - 06/25/2015 01:40 PM - Dmitry Moskalchuk

Beily Lan wrote:

> If you have time, please give us more detials for this bug, with next release version.

The problem was that whole stdio is re-implemented in libcrystax, but @popen@ was not included to the list, so @popen@ implementation was taken from bionic, while all other stdio functions from libcrystax (and FILE structures are not binary compatible between bionic and libcrystax). We've added @popen@ to the libcrystax too, so now it works fine. Just use recently published "10.2.0":https://www.crystax.net/android/ndk release, @popen@ is fixed there.

#8 - 07/01/2015 05:20 AM - Beily Lan

Dmitry Moskalchuk wrote:

> Beily Lan wrote:
>
> > If you have time, please give us more detials for this bug, with next release version.
>
> The problem was that whole stdio is re-implemented in libcrystax, but @popen@ was not included to the list, so @popen@ implementation was taken from bionic, while all other stdio functions from libcrystax (and FILE structures are not binary compatible between bionic and libcrystax). We've added @popen@ to the libcrystax too, so now it works fine. Just use recently published "10.2.0":https://www.crystax.net/android/ndk release, @popen@ is fixed there.

Thank you very much, Dmitry.

Files

MyApp002-popen-fread-crash-002.txt	19.7 KB	06/01/2015	Beily Lan
MyApp002-----.rar	806 KB	06/01/2015	Beily Lan
MyApp002.apk	881 KB	06/01/2015	Beily Lan