DESCRIPTION je...@gmail.com created issue #1 Sep 29, 20

Hi Supporter:

I tried the asan according to the below link on Android N:
https://source.android.com/devices/tech/debug/asan.html

I compiled the JNI lib according to the chapter: 'Building shared libraries with AddressSanitizer' and run the Android App which need this lib. But I always got the below error while starting this a

I build the same JNI lib and app with the NDK/SDK according to the below link and run this apk with the same device, it can work well and the issue in the code can be found by the asan.
May I get your help on this with high priority?

```
01-04 19:28:03.940  3137  3137 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
01-04 19:28:03.940  3137  3137 F DEBUG   : Build fingerprint: 'Android/msm8952_64/msm8952_64:7.0/NRD90M/zhanwe09021741:userdebug/test-keys'
01-04 19:28:03.940  3137  3137 F DEBUG   : Revision: '0'
01-04 19:28:03.940  3137  3137 F DEBUG   : ABI: 'arm64'
01-04 19:28:03.940  3137  3137 F DEBUG   : pid: 3122, tid: 3122, name: droid.simplejni  >>> com.example.android.simplejni <<<
01-04 19:28:03.940  3137  3137 F DEBUG   : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x0
01-04 19:28:03.940  3137  3137 F DEBUG   :    x0  000000000000000b x1  0000007fdd6a7818 x2  0000000000000000 x3  0000000000000000
01-04 19:28:03.940  3137  3137 F DEBUG   :    x4  ffffffffffffffff x5  0000000000000000 x6  0000000000000000 x7  5f636f6c6c616d5f
01-04 19:28:03.940  3137  3137 F DEBUG   :    x8  0000007f831d1000 x9  0000000048000004 x10 0000007f9e9bfad0 x11 0000000000000000
01-04 19:28:03.940  3137  3137 F DEBUG   :    x12 0000000000000000 x13 0000000000000000 x14 0000007fa1508000 x15 0000007fa1508000
01-04 19:28:03.940  3137  3137 F DEBUG   :    x16 0000007f82f7dec8 x17 0000007f9e966640 x18 00000000ffffffff x19 000000000000000b
01-04 19:28:03.940  3137  3137 F DEBUG   :    x20 0000007f82f4505c x21 463f890104145cc6 x22 0000001000000000 x23 463f890104145cc6
01-04 19:28:03.940  3137  3137 F DEBUG   :    x24 0000007f831d4000 x25 0000007f9c6f01b9 x26 0000001200000000 x27 0000001000000001
01-04 19:28:03.940  3137  3137 F DEBUG   :    x28 0000007f831d4000 x29 0000007fdd6a7800 x30 0000007f82f56d20
01-04 19:28:03.940  3137  3137 F DEBUG   :    sp  0000007fdd6a7800 pc  0000000000000000 pstate 0000000020000000
01-04 19:28:04.046  3137  3137 F DEBUG   :
01-04 19:28:04.046  3137  3137 F DEBUG   : backtrace:
01-04 19:28:04.046  3137  3137 F DEBUG   :    #00 pc 0000000000000000  <unknown>
01-04 19:28:04.046  3137  3137 F DEBUG   :    #01 pc 000000000007bd1c  /system/lib64/libclang_rt.asan-aarch64-android.so
01-04 19:28:04.046  3137  3137 F DEBUG   :    #02 pc 000000000007cfa8  /system/lib64/libclang_rt.asan-aarch64-android.so
01-04 19:28:04.046  3137  3137 F DEBUG   :    #03 pc 000000000007cef0  /system/lib64/libclang_rt.asan-aarch64-android.so
01-04 19:28:04.046  3137  3137 F DEBUG   :    #04 pc 0000000000070b28  /system/lib64/libclang_rt.asan-aarch64-android.so
01-04 19:28:04.046  3137  3137 F DEBUG   :    #05 pc 0000000000001334  /system/app/SimpleJNI/SimpleJNI.apk (offset 0x1000)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #06 pc 000000000000c4f4  /system/bin/linker64 (__dl__ZN6soinfo10call_arrayEPKcPPFvvEmb+360)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #07 pc 000000000000a50c  /system/bin/linker64 (__dl__Z9do_dlopenPKciPK17android_dlextinfoPv+540)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #08 pc 00000000000073f0  /system/bin/linker64 (__dl_android_dlopen_ext+60)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #09 pc 000000000000040c8  /system/lib64/libnativeloader.so (_ZN7android17OpenNativeLibraryEP7_JNIEnviPKcP8_jobjectP8_jstring+224)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #10 pc 00000000002ee38c  /system/lib64/libart.so
(_ZN3art9JavaVMExt17LoadNativeLibraryEP7_JNIEnvRKNSt3__112basic_stringIcNS3_11char_traitsIcEENS3_9allocatorIcEEEEP8_jobjectP8_jstringPS9_+1080)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #11 pc 000000000000427c  /system/lib64/libopenjdkjvm.so (JVM_NativeLoad+280)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #12 pc 000000000063ce20  /system/framework/arm64/boot.oat (offset 0x5a1000) (java.lang.Runtime.nativeLoad+204)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #13 pc 000000000063c8c0  /system/framework/arm64/boot.oat (offset 0x5a1000) (java.lang.Runtime.doLoad+204)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #14 pc 000000000063e6a0  /system/framework/arm64/boot.oat (offset 0x5a1000) (java.lang.Runtime.loadLibrary0+748)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #15 pc 0000000000659414  /system/framework/arm64/boot.oat (offset 0x5a1000) (java.lang.System.loadLibrary+96)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #16 pc 00000000000d1c68  /system/lib64/libart.so (art_quick_invoke_static_stub+600)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #17 pc 00000000000de6b0  /system/lib64/libart.so (_ZN3art9ArtMethod6InvokeEPNS_6ThreadEPjjPNS_6JValueEPKc+252)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #18 pc 000000000028c2e4  /system/lib64/libart.so
(_ZN3art11interpreter34ArtInterpreterToCompiledCodeBridgeEPNS_6ThreadEPNS_9ArtMethodEPKNS_7DexFile8CodeItemEPNS_11ShadowFrameEPNS_6JValueE+312)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #19 pc 00000000002852c0  /system/lib64/libart.so
(_ZN3art11interpreter6DoCallILb0ELb0EEEbPNS_9ArtMethodEPNS_6ThreadERNS_11ShadowFrameEPKNS_11InstructionEtPNS_6JValueE+592)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #20 pc 0000000000551c94  /system/lib64/libart.so (MterpInvokeStatic+356)
01-04 19:28:04.047  3137  3137 F DEBUG   :    #21 pc 00000000000c4514  /system/lib64/libart.so (ExecuteMterpImpl+14612)
```

Links (5)

" https://source.android.com/devices/tech/debug/asan.ht… "
"http://libclang_rt.asan-aarch64-android.so"
" … still haven't gotten ASAN for apps docs into any of the official sources, but the official ASAN docs are very good anyway: https://github.com/google/sanitizers/wiki/AddressSanitizerOnAndroid"
" https://source.android.com/devices/tech/debug/asan.html#building_shared_libraries_… "
"This was made much easier in O: https://developer.android.com/ndk/guides/asan"

COMMENTS All comments

je...@gmail.com <je...@gmail.com> #2 Sep 29, 201

By the way, I compiled a pure native linux application(with C language) with the whole android build together, it can work well and the asan also can find the memory issues correctly. It seems which loaded by the Android Application can't work.

en...@google.com <en...@google.com> Oct 5

Assigned to da...@google.com.

da...@google.com <da...@google.com> #3 Oct 5, 201

Those docs probably won't work for apps; they're intended for system libraries/services.

I believe we still haven't gotten ASAN for apps docs into any of the official sources, but the official ASAN docs are very good anyway: https://github.com/google/sanitizers/wiki/AddressSanit

One thing to note about their docs: they say you should set `NDK_TOOLCHAIN_VERSION := clang3.5`, for anything r11 or newer you actually want just "clang" (omit the version number).

Give that a shot and let us know if it fixes things. I'll take a look too once I find a moment.

je...@gmail.com <je...@gmail.com> #4 Oct 6, 201

Hi Danalb,

Thank you so much.
In fact, I've ever built the shared lib according to the below chapter:
https://source.android.com/devices/tech/debug/asan.html#building_shared_libraries_with_addresssanitizer

But I got the same issue(call stack) as I've mentioned previously.

je...@gmail.com <je...@gmail.com> #5 Oct 6, 201

The most strange thing is: why put the same apk and lib to /data/app and /system/app, the behavior are different.

da...@google.com <da...@google.com> #6 Oct 7, 201

You mean ASAN works if you install it to /system/app vs /data/app?

je...@gmail.com <je...@gmail.com> #7 Oct 8, 201

I mean it works if I install it to /data/app folder, but it can't work if I put the same app and *.so to /system/app.

je...@gmail.com <je...@gmail.com> #8 Oct 14, 201

Hi Danalb,

Are there any update on this case?

Thanks.
Jeffrey

da...@google.com <da...@google.com> #9 Oct 15, 201

Haven't had time to look at this yet.

da...@google.com <da...@google.com> #10 Oct 23, 201

Marked as fixed.

This was made much easier in O: https://developer.android.com/ndk/guides/asan