📁 Android Public Tracker   36991683 ▾

← C ☆ JNI ISSUE not able to track where is the segmentation fault i have also attached the log file   +1 2   Hotlists (1)   Mark as Duplicate   🔔 ⋮

Comments (5)   Dependencies   Duplicates (0)   Blocking (0)   Resources (1)

Infeasible   Bug   P4   + Add Hotlist   [AOSP] NotEnoughInformation

👥 **STATUS UPDATE** No update yet.   Edit

📄 DESCRIPTION an...@gmail.com created issue #1   Mar 15, 2014 07:39PM ⋮

```
03-13 19:02:12.820  5299  5299 F libc   : Fatal signal 11 (SIGSEGV) at 0x000005ec (code=1), thread 5299 (com.samsung.rcs)
03-13 19:02:12.875  1915  1915 I DEBUG  : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
03-13 19:02:12.875  1915  1915 I DEBUG  : Build fingerprint: 'samsung/m0xx/m0:4.2.2/JDQ39/M0_TEST:eng/test-keys'
03-13 19:02:12.875  1915  1915 I DEBUG  : Revision: '11'
03-13 19:02:12.875  1915  1915 I DEBUG  : pid: 5299, tid: 5299, name: com.samsung.rcs  >>> com.samsung.rcs <<<
03-13 19:02:12.875  1915  1915 I DEBUG  : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 000005ec
03-13 19:02:12.920  2301  2426 I InputReader: Touch event's action is 0x1 (deviceType=0) [pCnt=1, s=] when=50830072000
03-13 19:02:12.920  2301  2424 I InputDispatcher: Delivering touch to current input target: x: 312.000000, y: 1234.000000, action: 0x1, channel '42f99d40
com.samsung.rcs/com.samsung.rcs.UiVshMediaAppActivity (server)', toolType: 1
03-13 19:02:12.920  2301  2424 I InputDispatcher: Delivering touch to current input target: x: 312.000000, y: 1234.000000, action: 0x1, channel
'SamsungPolicyInputEventChannel (server)', toolType: 1
03-13 19:02:12.920  2301  2424 I InputDispatcher: Delivering touch to current input target: x: 312.000000, y: 1234.000000, action: 0x1, channel
'SamsungPolicyTouchInputEventToGestureChannel (server)', toolType: 1
03-13 19:02:12.920  2301  2424 I InputDispatcher: Delivering touch to current input target: x: 312.000000, y: 1234.000000, action: 0x1, channel 'TouchIntercepter (server)',
toolType: 1
03-13 19:02:12.935  2486  2486 D STATUSBAR-NetworkController: refreshSignalCluster: data=-1 bt=false
03-13 19:02:13.120  1915  1915 I DEBUG  :     r0 00000000  r1 000005e0  r2 579350f0  r3 59afc000
03-13 19:02:13.120  1915  1915 I DEBUG  :     r4 000005e0  r5 412e1f70  r6 00007c82  r7 0000005e
03-13 19:02:13.120  1915  1915 I DEBUG  :     r8 409b1480  r9 41dcefc8  sl 412b5f30  fp 00000001
03-13 19:02:13.120  1915  1915 I DEBUG  :     ip 104bfb5e  sp bef0f0a0  lr 409b312c  pc 409dbac0  cpsr 08000030
03-13 19:02:13.120  1915  1915 I DEBUG  :     d0  0000000000000000  d1  0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d2  0000000000000000  d3  0000046700000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d4  4304000043f18000  d5  000004533f800000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d6  44200000441c4000  d7  0000000044200000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d8  3f8000003f800000  d9  0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d10 0000000000000000  d11 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d12 0000000000000000  d13 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d14 0000000000000000  d15 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d16 7fffffffffffffff  d17 7fffffffffffffff
03-13 19:02:13.120  1915  1915 I DEBUG  :     d18 0000000000000000  d19 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d20 0000000000000000  d21 3fd5555560000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d22 0000000000000000  d23 3fd5555560000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d24 3ff0000000000000  d25 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d26 0000000000000000  d27 c038000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d28 0000000000000000  d29 3ff0000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     d30 3ff0000000000000  d31 3ff0000000000000
03-13 19:02:13.120  1915  1915 I DEBUG  :     scr 80000013
03-13 19:02:13.135  1915  1915 I DEBUG  :
```

📎 **deleted**   🔒 Restricted
   0 B ❓

✓ Links (1)   Hide all

"https://code.google.com/p/android-source-browsing/source/detail?repo=platform--dalvik&name=android-2.2.3_r2.1&r=ff1965e... "   bd...@ #3

COMMENTS   All comments ▼   ↓ Oldest first

⚪ **na...@google.com** <na...@google.com> #2   Mar 18, 2014 04:28AM ⋮
   Status: Won't Fix (Infeasible)

   There's really not enough information here. If you think this
   is a JNI issue, please turn on CheckJNI and try again.

   I took a look at our bug database and I couldn't find any other reports
   of this issue

⚪ **bd...@google.com** <bd...@google.com> #3   Mar 18, 2014 04:35AM ⋮

   They left off that this dying in dvmFindInterfaceMethodInCache. The only reference I could find here is an old 2.2 issue:

   https://code.google.com/p/android-source-browsing/source/detail?repo=platform--dalvik&name=android-2.2.3_r2.1&r=ff1965e61f4cfe0f31598945d751be2f3aa4b7f3

   So definitely need more information on how to reproduce on an AOSP device

Reporter

Type

Priority

Severity

Status

Access

Assignee

Verifier

Collaborato

CC

AOSP ID

ReportedBy

Found In

Targeted To

Verified In

In Prod

```
03-13 19:02:12.820  5299  5299 F libc    : Fatal signal 11 (SIGSEGV) at 0x000005ec (code=1), thread 5299 (com.samsung.rcs)
03-13 19:02:12.875  1915  1915 I DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
03-13 19:02:12.875  1915  1915 I DEBUG   : Build fingerprint: 'samsung/m0xx/m0:4.2.2/JDQ39/M0_TEST:eng/test-keys'
03-13 19:02:12.875  1915  1915 I DEBUG   : Revision: '11'
03-13 19:02:12.875  1915  1915 I DEBUG   : pid: 5299, tid: 5299, name: com.samsung.rcs  >>> com.samsung.rcs <<<
03-13 19:02:12.875  1915  1915 I DEBUG   : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 000005ec
03-13 19:02:12.920  2301  2426 I InputReader: Touch event's action is 0x1 (deviceType=0) [pCnt=1, s=] when=50830072000
03-13 19:02:12.920  2301  2424 I InputDispatcher: Delivering touch to current input target: x: 312.000000, y: 1234.000000, action: 0x1, channel '42f99d40
com.samsung.rcs/com.samsung.rcs.UiVshMediaAppActivity (server)', toolType: 1
03-13 19:02:12.920  2301  2424 I InputDispatcher: Delivering touch to current input target: x: 312.000000, y: 1234.000000, action: 0x1, channel
'SamsungPolicyInputEventChannel (server)', toolType: 1
03-13 19:02:12.920  2301  2424 I InputDispatcher: Delivering touch to current input target: x: 312.000000, y: 1234.000000, action: 0x1, channel
'SamsungPolicyTouchInputEventToGestureChannel (server)', toolType: 1
03-13 19:02:12.920  2301  2424 I InputDispatcher: Delivering touch to current input target: x: 312.000000, y: 1234.000000, action: 0x1, channel 'TouchIntercepter
(server)', toolType: 1
03-13 19:02:12.935  2486  2486 D STATUSBAR-NetworkController: refreshSignalCluster: data=-1 bt=false
03-13 19:02:13.120  1915  1915 I DEBUG   :     r0 00000000  r1 000005e0  r2 579350f0  r3 59afc000
03-13 19:02:13.120  1915  1915 I DEBUG   :     r4 000005e0  r5 412e1f70  r6 00007c82  r7 0000005e
03-13 19:02:13.120  1915  1915 I DEBUG   :     r8 409b1480  r9 41dcefc8  sl 412b5f30  fp 00000001
03-13 19:02:13.120  1915  1915 I DEBUG   :     ip 104bfb5e  sp bef0f0a0  lr 409b312c  pc 409dbac0  cpsr 08000030
03-13 19:02:13.120  1915  1915 I DEBUG   :     d0  0000000000000000  d1  0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d2  0000000000000000  d3  0000046700000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d4  4304000043f18000  d5  000004533f800000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d6  44200000441c4000  d7  0000000044200000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d8  3f8000003f800000  d9  0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d10 0000000000000000  d11 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d12 0000000000000000  d13 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d14 0000000000000000  d15 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d16 7fffffffffffffff  d17 7fffffffffffffff
03-13 19:02:13.120  1915  1915 I DEBUG   :     d18 0000000000000000  d19 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d20 0000000000000000  d21 3fd5555560000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d22 0000000000000000  d23 3fd5555560000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d24 3ff0000000000000  d25 0000000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d26 0000000000000000  d27 c038000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d28 0000000000000000  d29 3ff0000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     d30 3ff0000000000000  d31 3ff0000000000000
03-13 19:02:13.120  1915  1915 I DEBUG   :     scr 80000013
03-13 19:02:13.135  1915  1915 I DEBUG   :
03-13 19:02:13.135  1915  1915 I DEBUG   : backtrace:
03-13 19:02:13.135  1915  1915 I DEBUG   :     #00  pc 00048ac0  /system/lib/libdvm.so (dvmFindInterfaceMethodInCache+23)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #01  pc 00020128  /system/lib/libdvm.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #02  pc 0002b604  /system/lib/libdvm.so (dvmInterpret(Thread*, Method const*, JValue*)+184)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #03  pc 0005fd31  /system/lib/libdvm.so (dvmCallMethodV(Thread*, Method const*, Object*, bool, JValue*,
std::__va_list)+272)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #04  pc 0004c3b5  /system/lib/libdvm.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #05  pc 0003fda9  /system/lib/libdvm.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #06  pc 0004e7a5  /system/lib/libandroid_runtime.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #07  pc 0005f5e7  /system/lib/libandroid_runtime.so (android::NativeInputEventReceiver::consumeEvents(_JNIEnv*, bool,
long long)+250)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #08  pc 0005f6fd  /system/lib/libandroid_runtime.so (android::NativeInputEventReceiver::handleEvent(int, int, void*)+92)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #09  pc 00014ec5  /system/lib/libutils.so (android::Looper::pollInner(int)+516)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #10  pc 00014f89  /system/lib/libutils.so (android::Looper::pollOnce(int, int*, int*, void**)+104)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #11  pc 0006478f  /system/lib/libandroid_runtime.so (android::NativeMessageQueue::pollOnce(_JNIEnv*, int)+22)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #12  pc 0001e310  /system/lib/libdvm.so (dvmPlatformInvoke+112)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #13  pc 0004d511  /system/lib/libdvm.so (dvmCallJNIMethod(unsigned int const*, JValue*, Method const*,
Thread*)+396)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #14  pc 00038c8d  /system/lib/libdvm.so (dvmCheckCallJNIMethod(unsigned int const*, JValue*, Method const*,
Thread*)+8)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #15  pc 00027720  /system/lib/libdvm.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #16  pc 0002b604  /system/lib/libdvm.so (dvmInterpret(Thread*, Method const*, JValue*)+184)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #17  pc 00060007  /system/lib/libdvm.so (dvmInvokeMethod(Object*, Method const*, ArrayObject*, ArrayObject*,
ClassObject*, bool)+374)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #18  pc 00067931  /system/lib/libdvm.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #19  pc 00027720  /system/lib/libdvm.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #20  pc 0002b604  /system/lib/libdvm.so (dvmInterpret(Thread*, Method const*, JValue*)+184)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #21  pc 0005fd31  /system/lib/libdvm.so (dvmCallMethodV(Thread*, Method const*, Object*, bool, JValue*,
std::__va_list)+272)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #22  pc 00049a83  /system/lib/libdvm.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #23  pc 0003cfe3  /system/lib/libdvm.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #24  pc 0004b7bb  /system/lib/libandroid_runtime.so
03-13 19:02:13.135  1915  1915 I DEBUG   :     #25  pc 0004cb57  /system/lib/libandroid_runtime.so (android::AndroidRuntime::start(char const*, char const*)+390)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #26  pc 00000db7  /system/bin/app_process
03-13 19:02:13.135  1915  1915 I DEBUG   :     #27  pc 0001276f  /system/lib/libc.so (__libc_init+38)
03-13 19:02:13.135  1915  1915 I DEBUG   :     #28  pc 00000ae8  /system/bin/app_process
```

---

an...@gmail.com <an...@gmail.com> #4   Mar 19, 2014 04:10PM ⋮

If there is so issue then how can the app crash This is the log that i have watelse is required

---

bd...@google.com <bd...@google.com> #5   Mar 19, 2014 04:51PM ⋮

Without steps to reproduce in AOSP or a stack from Google device image where we have symbols, there is not much we can do. It looks like this is an internal Samsung
build: samsung/m0xx/m0:4.2.2/JDQ39/M0_TEST:eng/test-keys and for all we know local changes are causing the issue.