5.1: crash in ART while debugging

+1 4 Hotlists (1) Mark as Duplicate

Comments (7) Dependencies Duplicates (0) Blocking (0) Resources (3)

Obsolete Bug P3 + Add Hotlist [AOSP] assigned

STATUS UPDATE No update yet. Edit

DESCRIPTION km...@gmail.com created issue #1

Nexus 5, 5.1/LMY47D/1743759:user/release-keys

I was just debugging along, when my app crashed inside ART.

```
The output of "adb bugreport" is attached.-20 22:57:41.570 F/libc    ( 8835): Fatal signal 6 (SIGABRT), code -6 in tid 8845 (JDWP)
03-20 22:57:41.659 I/DEBUG  (  184): *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
03-20 22:57:41.661 I/DEBUG  (  184): Build fingerprint: 'google/hammerhead/hammerhead:5.1/LMY47D/1743759:user/release-keys'
03-20 22:57:41.661 I/DEBUG  (  184): Revision: '11'
03-20 22:57:41.661 I/DEBUG  (  184): ABI: 'arm'
03-20 22:57:41.661 I/DEBUG  (  184): pid: 8835, tid: 8845, name: JDWP  >>> org.kman.AquaMail <<<
03-20 22:57:41.661 I/DEBUG  (  184): signal 6 (SIGABRT), code -6 (SI_TKILL), fault addr --------
03-20 22:57:41.690 I/DEBUG  (  184): Abort message: 'art/runtime/debugger.cc:2630] Register 0 expected to hold JT_OBJECT object: 0x134fc0a0'
03-20 22:57:41.690 I/DEBUG  (  184):     r0 00000000  r1 0000228d  r2 00000006  r3 00000000
03-20 22:57:41.690 I/DEBUG  (  184):     r4 b3e72db8  r5 00000006  r6 0000000b  r7 0000010c
03-20 22:57:41.690 I/DEBUG  (  184):     r8 00000001  r9 b486f520  sl aec41400  fp aec31700
03-20 22:57:41.690 I/DEBUG  (  184):     ip 0000228d  sp b3e72450  lr b6db03c5  pc b6dd3c80  cpsr 60070010
03-20 22:57:41.691 I/DEBUG  (  184):
03-20 22:57:41.691 I/DEBUG  (  184): backtrace:
03-20 22:57:41.691 I/DEBUG  (  184):     #00 pc 0003ac80  /system/lib/libc.so (tgkill+12)
03-20 22:57:41.691 I/DEBUG  (  184):     #01 pc 000173c1  /system/lib/libc.so (pthread_kill+52)
03-20 22:57:41.691 I/DEBUG  (  184):     #02 pc 00017fd3  /system/lib/libc.so (raise+10)
03-20 22:57:41.691 I/DEBUG  (  184):     #03 pc 00014795  /system/lib/libc.so (__libc_android_abort+36)
03-20 22:57:41.691 I/DEBUG  (  184):     #04 pc 00012f44  /system/lib/libc.so (abort+4)
03-20 22:57:41.691 I/DEBUG  (  184):     #05 pc 00228cd7  /system/lib/libart.so (art::Runtime::Abort()+170)
03-20 22:57:41.691 I/DEBUG  (  184):     #06 pc 000a7371  /system/lib/libart.so (art::LogMessage::~LogMessage()+1360)
03-20 22:57:41.691 I/DEBUG  (  184):     #07 pc 000f49b1  /system/lib/libart.so (art::Dbg::GetLocalValue(art::StackVisitor const&, art::ScopedObjectAccessUnchecked&, int, art::JDWP::JdwpTag,
03-20 22:57:41.691 I/DEBUG  (  184):     #08 pc 000f53c3  /system/lib/libart.so (art::Dbg::GetLocalValues(art::JDWP::Request*, art::JDWP::ExpandBuf*)+614)
03-20 22:57:41.691 I/DEBUG  (  184):     #09 pc 001993fb  /system/lib/libart.so (art::JDWP::JdwpState::ProcessRequest(art::JDWP::Request&, art::JDWP::ExpandBuf*)+418)
03-20 22:57:41.691 I/DEBUG  (  184):     #10 pc 0019b69f  /system/lib/libart.so (art::JDWP::JdwpState::HandlePacket()+62)
03-20 22:57:41.692 I/DEBUG  (  184):     #11 pc 00298dff  /system/lib/libart.so (art::JDWP::JdwpAdbState::ProcessIncoming()+1050)
03-20 22:57:41.692 I/DEBUG  (  184):     #12 pc 0019c015  /system/lib/libart.so (art::JDWP::JdwpState::Run()+356)
03-20 22:57:41.692 I/DEBUG  (  184):     #13 pc 0019d561  /system/lib/libart.so (art::JDWP::StartJdwpThread(void*)+16)
03-20 22:57:41.692 I/DEBUG  (  184):     #14 pc 00016baf  /system/lib/libc.so (__pthread_start(void*)+30)
03-20 22:57:41.692 I/DEBUG  (  184):     #15 pc 00014af3  /system/lib/libc.so (__start_thread+6)
```

deleted
0 B ?

✓ Links (3)

“(https://android.googlesource.com/platform/art/+/master/runtim…)”
“ …e of invalid object is an incorrect use of JNI references. Does your app execute JNI code from a library? You may want to enable CheckJNI to be sure your app is JNI safe: http://developer.android.c
“FYI https://android-review.googlesource.com/143988 provides better error reporting, including invalid object access.”

COMMENTS

en...@google.com <en...@google.com>

Assigned to sh...@google.com.

sh...@google.com <sh...@google.com> #2

Thank you for the report.

According to the abort message, it appears the debugger asks to read an object value in DEX register v0. However the object 0x134fc0a0 in this register is invalid. Here's the code in ART:

```
if (!Runtime::Current()->GetHeap()->IsValidObjectAddress(o)) {
  LOG(FATAL) << "Register " << reg << " expected to hold " << tag << " object: " << o;
}
```
(https://android.googlesource.com/platform/art/+/master/runtime/debugger.cc)

One famous cause of invalid object is an incorrect use of JNI references. Does your app execute JNI code from a library? You may want to enable CheckJNI to be sure your app is JNI safe: h

The abort message itself is not very valuable here. I'll change it to be clear about why the runtime crashes and where that happens (method, DEX pc, ...).

km...@gmail.com <km...@gmail.com> #3

Nope, there is no JNI in my code.

I should mention that the debugger is Eclipse, but before you tell me that Eclipse is deprecated -- I've never seen any such crashes with Android 1.6 - 4.4, Dalvik runtime.

ag...@google.com <ag...@google.com> #4

Please attach the APK you're testing and reproduction steps (as in, which method is being debugged when ART aborts).

You may also send it directly to shertz (at) google.com.

km...@gmail.com <km...@gmail.com> #5

I'll be sure to do it next time it happens. It has happened before so I assume it will happen again, just may take a while. Thank you for the email address.

ag...@google.com <ag...@google.com> #6

Your help is very much appreciated.

sh...@google.com <sh...@google.com> #7

FYI https://android-review.googlesource.com/143988 provides better error reporting, including invalid object access.

sh...@google.com <sh...@google.com>

Status: Won't Fix (Obsolete)