[Tiramisu] Bug-9: ART crashed with return code 134

+1 6 Hotlists (4) Mark as Duplicate

Comments (5) Dependencies Duplicates (0) Blocking (0) Resources (2)

Fixed Bug P3 + Add Hotlist Platform adexe s nau

STATUS UPDATE No update yet. Edit

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

The `Test.java` in the enclosed archive crashed ART with the following log:

```
03-30 14:28:54.337  7261  7261 F libc    : Fatal signal 6 (SIGABRT), code -1 (SI_QUEUE) in tid 7261 (main), pid 7261 (main)
03-30 14:28:54.696  7275  7275 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
03-30 14:28:54.696  7275  7275 F DEBUG   : Build fingerprint: 'google/sdk_gphone64_x86_64/emu64xa:Tiramisu/TPP2.220218.008/8250781:userdebug/dev-keys'
03-30 14:28:54.696  7275  7275 F DEBUG   : Revision: '0'
03-30 14:28:54.696  7275  7275 F DEBUG   : ABI: 'x86_64'
03-30 14:28:54.696  7275  7275 F DEBUG   : Timestamp: 2022-03-30 14:28:54.426173778+0200
03-30 14:28:54.696  7275  7275 F DEBUG   : Process uptime: 3s
03-30 14:28:54.696  7275  7275 F DEBUG   : Cmdline: dalvikvm -cp /data/local/tmp/test.jar Test
03-30 14:28:54.696  7275  7275 F DEBUG   : pid: 7261, tid: 7261, name: main  >>> dalvikvm <<<
03-30 14:28:54.696  7275  7275 F DEBUG   : uid: 0
03-30 14:28:54.696  7275  7275 F DEBUG   : signal 6 (SIGABRT), code -1 (SI_QUEUE), fault addr --------
03-30 14:28:54.697  7275  7275 F DEBUG   : Abort message: 'GC tried to mark invalid reference 0x1
03-30 14:28:54.697  7275  7275 F DEBUG   : ref=0x1 <invalid address>
...
03-30 14:28:54.697  7275  7275 F DEBUG   : backtrace:
03-30 14:28:54.697  7275  7275 F DEBUG   :       #00 pc 000000000005ecef  /apex/com.android.runtime/lib64/bionic/libc.so (abort+191) (BuildId: 4a49f5f713524c
03-30 14:28:54.697  7275  7275 F DEBUG   :       #01 pc 00000000007ed1c4  /apex/com.android.art/lib64/libart.so (art::Runtime::Abort(char const*)+1124) (Buil
03-30 14:28:54.697  7275  7275 F DEBUG   :       #02 pc 0000000000019a8c  /apex/com.android.art/lib64/libbase.so (android::base::SetAborter(std::__1::functio
03-30 14:28:54.697  7275  7275 F DEBUG   :       #03 pc 0000000000018fde  /apex/com.android.art/lib64/libbase.so (android::base::LogMessage::~LogMessage()+35
03-30 14:28:54.697  7275  7275 F DEBUG   :       #04 pc 000000000054f60c  /apex/com.android.art/lib64/libart.so (art::gc::Verification::LogHeapCorruption(art
03-30 14:28:54.697  7275  7275 F DEBUG   :       #05 pc 00000000004c7ce6  /apex/com.android.art/lib64/libart.so (art::gc::collector::ConcurrentCopying::MarkN
03-30 14:28:54.697  7275  7275 F DEBUG   :       #06 pc 00000000004ca4f8  /apex/com.android.art/lib64/libart.so (art::gc::collector::ConcurrentCopying::Threa
03-30 14:28:54.697  7275  7275 F DEBUG   :       #07 pc 000000000086ac32  /apex/com.android.art/lib64/libart.so (art::ReferenceMapVisitor<art::RootCallbackVi
03-30 14:28:54.697  7275  7275 F DEBUG   :       #08 pc 0000000000817db8  /apex/com.android.art/lib64/libart.so (void art::StackVisitor::WalkStack<(art::Stac
03-30 14:28:54.697  7275  7275 F DEBUG   :       #09 pc 0000000000861ad1  /apex/com.android.art/lib64/libart.so (art::Thread::VisitRoots(art::RootVisitor*, a
03-30 14:28:54.697  7275  7275 F DEBUG   :       #10 pc 00000000004ca21d  /apex/com.android.art/lib64/libart.so (art::gc::collector::ConcurrentCopying::Threa
03-30 14:28:54.697  7275  7275 F DEBUG   :       #11 pc 0000000000856a39  /apex/com.android.art/lib64/libart.so (art::Thread::FullSuspendCheck(bool)+1225) (B
03-30 14:28:54.697  7275  7275 F DEBUG   :       #12 pc 0000000000922f0b  /apex/com.android.art/lib64/libart.so (artTestSuspendFromCode+43) (BuildId: f9c2294
03-30 14:28:54.697  7275  7275 F DEBUG   :       #13 pc 000000000037b20d  /apex/com.android.art/lib64/libart.so (art_quick_test_suspend+173) (BuildId: f9c229
03-30 14:28:54.697  7275  7275 F DEBUG   :       #14 pc 000000002001ca8  /memfd:jit-cache (deleted) (java.lang.ArrayIndexOutOfBoundsException.<init>+216)
03-30 14:28:54.697  7275  7275 F DEBUG   :       #15 pc 0000000000371cb4  /apex/com.android.art/lib64/libart.so (art_quick_invoke_stub+756) (BuildId: f9c2294
03-30 14:28:54.697  7275  7275 F DEBUG   :       #16 pc 00000000003f1a16  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigne
03-30 14:28:54.697  7275  7275 F DEBUG   :       #17 pc 00000000007e56c1  /apex/com.android.art/lib64/libart.so (art::JValue art::InvokeWithJValues<art::ArtM
03-30 14:28:54.697  7275  7275 F DEBUG   :       #18 pc 000000000085fc43  /apex/com.android.art/lib64/libart.so (art::Thread::ThrowNewWrappedException(char c
03-30 14:28:54.697  7275  7275 F DEBUG   :       #19 pc 0000000000467727  /apex/com.android.art/lib64/libart.so (art::ThrowException(char const*, art::ObjPtr
03-30 14:28:54.697  7275  7275 F DEBUG   :       #20 pc 00000000004678d5  /apex/com.android.art/lib64/libart.so (art::ThrowArrayIndexOutOfBoundsException(int
03-30 14:28:54.697  7275  7275 F DEBUG   :       #21 pc 00000000009230a8  /apex/com.android.art/lib64/libart.so (artThrowArrayBoundsFromCode+8) (BuildId: f9c
03-30 14:28:54.697  7275  7275 F DEBUG   :       #22 pc 000000000037120d  /apex/com.android.art/lib64/libart.so (art_quick_throw_array_bounds+173) (BuildId:
03-30 14:28:54.697  7275  7275 F DEBUG   :       #23 pc 0000000002001b72  /memfd:jit-cache (deleted) (Test.vMeth1+2898)
03-30 14:28:54.698  7275  7275 F DEBUG   :       #24 pc 0000000000368428  /apex/com.android.art/lib64/libart.so (nterp_helper+56) (BuildId: f9c22944c82b378b1
03-30 14:28:54.698  7275  7275 F DEBUG   :       #25 pc 0000000000002176  [anon:dalvik-classes.dex extracted in memory from /data/local/tmp/test.jar] (Test.v
03-30 14:28:54.698  7275  7275 F DEBUG   :       #26 pc 0000000000368428  /apex/com.android.art/lib64/libart.so (nterp_helper+56) (BuildId: f9c22944c82b378b1
03-30 14:28:54.698  7275  7275 F DEBUG   :       #27 pc 0000000000001a7e  [anon:dalvik-classes.dex extracted in memory from /data/local/tmp/test.jar] (Test.b
03-30 14:28:54.698  7275  7275 F DEBUG   :       #28 pc 0000000000368428  /apex/com.android.art/lib64/libart.so (nterp_helper+56) (BuildId: f9c22944c82b378b1
03-30 14:28:54.698  7275  7275 F DEBUG   :       #29 pc 0000000000001c42  [anon:dalvik-classes.dex extracted in memory from /data/local/tmp/test.jar] (Test.m
03-30 14:28:54.698  7275  7275 F DEBUG   :       #30 pc 0000000000369288  /apex/com.android.art/lib64/libart.so (nterp_helper+3736) (BuildId: f9c22944c82b378
03-30 14:28:54.698  7275  7275 F DEBUG   :       #31 pc 0000000000001be0  [anon:dalvik-classes.dex extracted in memory from /data/local/tmp/test.jar] (Test.m
03-30 14:28:54.698  7275  7275 F DEBUG   :       #32 pc 0000000000372016  /apex/com.android.art/lib64/libart.so (art_quick_invoke_static_stub+806) (BuildId:
03-30 14:28:54.698  7275  7275 F DEBUG   :       #33 pc 00000000003f1a49  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigne
03-30 14:28:54.698  7275  7275 F DEBUG   :       #34 pc 00000000007e4fc1  /apex/com.android.art/lib64/libart.so (art::JValue art::InvokeWithVarArgs<art::ArtM
03-30 14:28:54.698  7275  7275 F DEBUG   :       #35 pc 0000000000644a74  /apex/com.android.art/lib64/libart.so (art::JNI<false>::CallStaticVoidMethodV(_JNIE
03-30 14:28:54.698  7275  7275 F DEBUG   :       #36 pc 0000000000002a84  /apex/com.android.art/bin/dalvikvm64 (_JNIEnv::CallStaticVoidMethod(_jclass*, _jmet
03-30 14:28:54.698  7275  7275 F DEBUG   :       #37 pc 000000000000271c  /apex/com.android.art/bin/dalvikvm64 (art::dalvikvm(int, char**)+2060) (BuildId: c4
03-30 14:28:54.698  7275  7275 F DEBUG   :       #38 pc 0000000000001ef5  /apex/com.android.art/bin/dalvikvm64 (main+5) (BuildId: c4b9abdc3d0244c2262af6c81d3
03-30 14:28:54.698  7275  7275 F DEBUG   :       #39 pc 00000000000505f9  /apex/com.android.runtime/lib64/bionic/libc.so (__libc_init+89) (BuildId: 4a49f5f71
```

Environment to reproduce the problem

Android Build: Tiramisu; TPP2.220218.008

```
$ adb shell getprop ro.system.build.id
TPP2.220218.008
```

Android Build Tools: bulid-tools;33.0.0-rc2

```
$ ./build-tools/33.0.0-rc2/d8 --version
D8 3.3.11-dev (build 5d015d7a69cc8b662b4f28a71ff2a4dfd5adc1bb from go/r8bot (luci-r8-custom-ci-xenial-13-fsvv))
```

HotSpot and OpenJDK: java-11-openjdk-amd64

```
$ java -version
openjdk version "11.0.14" 2022-01-18
OpenJDK Runtime Environment (build 11.0.14+9-Ubuntu-0ubuntu2.20.04)
OpenJDK 64-Bit Server VM (build 11.0.14+9-Ubuntu-0ubuntu2.20.04, mixed mode, sharing)
$ javac -version
javac 11.0.14
```

Please also check the following link for the bugreport (of `adb bugreport`): https://drive.google.com/file/d/19kFtWEGihzj_8M7NyvFntLrAl7K_1vhg/view?usp=sharing

We have already shared the above bugreport with android-bugreport@google.com.

Steps to reproduce the problem (including sample code if appropriate)

> Note, `Test.class` and `test.jar` are precompiled using `javac` and `d8` as aforementioned

Push `test.jar` to the emulator

```
$ adb push test.jar /data/local/tmp/
```

Run in dalvikvm

```
$ adb shell dalvikvm -cp /data/local/tmp/test.jar Test
```

Check the return code

```
$ echo $?
```

What happened

ART crashed with return code 134

What you think the correct behavior should be

ART does not crash

deleted

0 B

COMMENTS

ad...@google.com <ad...@google.com>

Assigned to ad...@google.com.

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

We have passed this to the development team and will update this issue with more information as it becomes available.

ad...@google.com <ad...@google.com> #3

Marked as fixed.

The issue has been fixed and it will be available in a future build.

fe...@gmail.com <fe...@gmail.com> #4

Hi google team,
Could you share the patch about this bug? thanks.

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

Please give us a patch, we have the problem yet