





Sign in

☐ Android Public Tracker > Android 14 Developer Preview / Beta 229134124 ▼

← C ☆ [Tiramisu] Bug-41: ART Crashed with JNI Error: Global Reference Table Overflow (Exit Code: 134)

3 Hotlists (4) Mark as Duplicate

plicate 🗘

Comments (3) Dependencies Duplicates (0) Blocking (0) Resources (2)

Fixed Bug P3 + Add Hotlist Platform adexes 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:

04-14 13:02:36.774 756 756 F libc : Fatal signal 6 (SIGABRT), code -1 (SI_QUEUE) in tid 756 (main), pid 756 (main) 04-14 13:02:37.357 1706 1706 F DEBUG 04-14 13:02:37, 357 1706 1706 F DEBUG : Build fingerprint: 'google/sdk_gphone64_x86_64/emu64xa:Tiramisu/TPP2.220218.008/8250781:userdebug/dev-keys' 04-14 13:02:37.357 1706 1706 F DEBUG : Revision: '0' 04-14 13:02:37.357 1706 1706 F DEBUG : ABI: 'x86_64' : Timestamp: 2022-04-14 13:02:36.853176746+0200 04-14 13:02:37.357 1706 1706 F DEBUG 04-14 13:02:37.357 1706 1706 F DEBUG : Process uptime: 36s 04-14 13:02:37.357 1706 1706 F DEBUG : Cmdline: dalvikvm -cp /data/local/tmp/test.jar Test 04-14 13:02:37, 357 1706 1706 F DEBUG : pid: 756, tid: 756, name: main >>> dalvikvm <<< 04-14 13:02:37.357 1706 1706 F DEBUG : uid: 2000 : signal 6 (SIGABRT), code -1 (SI_QUEUE), fault addr -----04-14 13:02:37.358 1706 F DEBUG 04-14 13:02:37.358 1706 1706 F DEBUG : Abort message: 'JNI ERROR (app bug): global reference table overflow (max=51200) global reference table dump: 04-14 13:02:37, 358 1706 1706 F DEBUG Last 10 entries (of 51200): 04-14 13:02:37.358 1706 1706 F DEBUG 51199: 0x12e40348 java.lang.Class<Test> 04-14 13:02:37.358 1706 1706 F DEBUG 51198: 0x12e40348 java.lang.Class<Test> 51197: 0x12e40348 java.lang.Class<Test> 1706 F DEBUG 04-14 13:02:37, 358 1706 04-14 13:02:37.358 1706 1706 F DEBUG 51196: 0x12e40348 java.lang.Class<Test> 1706 F DEBUG 51195: 0x12e40348 java.lang.Class<Test> 04-14 13:02:37.358 1706 04-14 13:02:37.358 1706 1706 F DEBUG 51194: 0x12e40348 java.lang.Class(Test) 1706 51193: 0x12e40348 java.lang.Class<Test> 04-14 13:02:37.358 1706 F DEBUG 04-14 13:02:37.358 1706 1706 F DEBUG 51192: 0x12e40348 java.lang.Class<Test> 04-14 13:02:37, 358 1706 1706 F DEBUG 51191: 0x12e40348 java.lang.Class<Test> 04-14 13:02:37.358 1706 1706 F DEBUG 51190: 0x12e40348 java, lang, Class<Test> 04-14 13:02:37.358 1706 F DEBUG Summary: 1706 F DEBUG $04\text{-}14\ 13\text{:}02\text{:}37\text{.}358$ 1706 51196 of java.lang.Class (84 unique instances) 2 of dalvik.system.PathClassLoader (1 unique instances) 04-14 13:02:37, 358 1706 1706 F DEBUG 04-14 13:02:37.358 1706 1706 F DEBUG 2 of java.lang.ThreadGroup (2 unique instances) 04-14 13:02:37.358 1706 1706 F DEBUG rax 000000000000000 rbx 0000000000002f4 rcx 00007b45962e4cef rdx 0000000000000000 1706 F DEBUG r8 00007b43a60fb391 r9 00007b43a60fb391 r10 00007ffc27eed710 r11 0000000000000217 04-14 13:02:37, 358 1706 04-14 13:02:37.358 1706 1706 F DEBUG rl2 000000000000000 rl3 00000005a000000 rl4 00007ffc27eed708 rl5 00000000000002f4 rdi 00000000000002f4 rsi 00000000000002f4 04-14 13:02:37.358 1706 1706 F DEBUG 1706 F DEBUG 04-14 13:02:37.358 1706 rbp 00007b44460d0010 rsp 00007ffc27eed700 rip 00007b45962e4cef 1706 04-14 13:02:37.358 1706 F DEBUG : backtrace: /apex/com.android.runtime/lib64/bionic/libc.so (abort+191) (BuildId: 4a49f5f713524c 04-14 13:02:37.358 1706 1706 F DEBUG #00 pc 000000000005ecef 04-14 13:02:37, 358 1706 1706 F DEBUG #01 pc 00000000007ed1c4 /apex/com.android.art/lib64/libart.so (art::Runtime::Abort(char const*)+1124) (Buil 04-14 13:02:37, 358 1706 1706 F DEBUG #02 pc 0000000000019a8c /apex/com, android.art/lib64/libbase.so (android::base::SetAborter(std:: 1::functio 04-14 13:02:37.358 1706 F DEBUG #03 pc 000000000018fde /apex/com.android.art/lib64/libbase.so (android::base::LogMessage::~LogMessage()+35 $04\text{-}14\ 13\text{:}02\text{:}37\text{.}358$ 1706 1706 F DEBUG #04 pc 00000000005fa8d2 /apex/com.android.art/lib64/libart.so (art::JavaVMExt::AddGlobalRef(art::Thread*, a 04-14 13:02:37, 358 1706 1706 F DEBUG #05 pc 00000000005adf3b /apex/com.android.art/lib64/libart.so (art::jit::JitCompileTask::JitCompileTask(art 04-14 13:02:37.358 1706 1706 F DEBUG #06 pc 00000000005b1ad5 /apex/com.android.art/lib64/libart.so (art::jit::Jit::EnqueueCompilation(art::ArtMe 04-14 13:02:37.358 1706 1706 F DEBUG #07 pc 000000000093c124 /apex/com.android.art/lib64/libart.so (NterpHotMethod+244) (BuildId: f9c22944c82b37 04-14 13:02:37, 358 1706 1706 F DEBUG #08 pc 00000000036f499 /apex/com.android.art/lib64/libart.so (nterp_hot_method+73) (BuildId: f9c22944c82b3 04-14 13:02:37.358 1706 1706 F DEBUG #09 pc 000000000036e34b /apex/com.android.art/lib64/libart.so (nterp_helper+24411) (BuildId: f9c22944c82b37 #10 pc 0000000000000dec [anon:dalvik-classes.dex extracted in memory from /data/local/tmp/test.jar] (Test.t 04-14 13:02:37.358 1706 1706 F DEBUG 04-14 13:02:37.358 1706 1706 F DEBUG #11 pc 0000000000369288 /apex/com.android.art/lib64/libart.so (nterp_helper+3736) (BuildId: f9c22944c82b378 04-14 13:02:37.358 1706 1706 F DEBUG #12 pc 0000000000007014 [anon:dalvik-classes.dex extracted in memory from /data/local/tmp/test.jar] (Test.m 04-14 13:02:37.358 1706 1706 F DEBUG #13 pc 0000000000372016 /apex/com.android.art/lib64/libart.so (art_quick_invoke_static_stub+806) (BuildId: 04-14 13:02:37.358 1706 1706 F DEBUG #14 pc 00000000003f1a49 /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigne 04-14 13:02:37, 358 1706 1706 F DEBUG #15 pc 00000000007e4fc1 /apex/com, android, art/lib64/libart, so (art::IValue art::InvokeWithVarArgs<art::ArtM 04-14 13:02:37.358 1706 1706 F DEBUG #16 pc 0000000000644a74 /apex/com.android.art/lib64/libart.so (art::JNI<false>::CallStaticVoidMethodV(_JNIE $04\text{-}14\ 13\text{:}02\text{:}37\text{.}358$ 1706 1706 F DEBUG #17 pc 00000000000002a84 /apex/com.android.art/bin/dalvikvm64 (_JNIEnv::CallStaticVoidMethod(_jclass*, _jmet 04-14 13:02:37, 358 1706 1706 F DEBUG #18 pc 0000000000000271c /apex/com.android.art/bin/dalvikvm64 (art::dalvikvm(int, char**)+2060) (BuildId: c4 04-14 13:02:37.358 1706 1706 F DEBUG #19 pc 0000000000001ef5 /apex/com.android.art/bin/dalvikvm64 (main+5) (BuildId: c4b9abdc3d0244c2262af6c81d3 #20 pc 0000000000505f9 04-14 13:02:37.358 1706 1706 F DEBUG /apex/com.android.runtime/lib64/bionic/libc.so (__libc_init+89) (BuildId: 4a49f5f71

 $Please also \ check \ the following \ link for \ the \ buggeport (of adb \ buggeport): \ https://drive.google.com/file/d/19nXs2GzqsG8UlxRZ_9rJ5BnOxYRFyxWq/view?usp=sharing \ buggeport (of adb \ buggeport): \ https://drive.google.com/file/d/19nXs2GzqsG8UlxRZ_9$

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

```
$ adb shell getprop ro.system.build.id
      TPP2. 220218. 008
    Android Build Tools: bulid-tools;33.0.0-rc2
      D8~3.~3.~11-dev~(build~5d015d7a69cc8b662b4f28a71ff2a4dfd5adclbb~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-Oubuntu2.20.04)
      OpenJDK 64-Bit Server VM (build 11.0.14+9-Ubuntu-Oubuntu2.20.04, mixed mode, sharing)
      $ javac -version
      javac 11.0.14
    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
     (i) deleted
         0B (?)
COMMENTS
        an...@gmail.com <an...@gmail.com><u>#2</u>
        Note, there is a large but quite simple loop (Line 91-122) in Test. java. If you comment this loop, the test won't crash ART.
        ve...@google.com <ve...@google.com>
        Assigned to ve...@google.com.
        ve...@google.com <ve...@google.com>
        Assigned to ve...@google.com.
        ve...@google.com < ve...@google.com > \underline{\#3}
        Marked as fixed.
        The issue has been fixed and it will be available in a future build.
```