← ↻ ☆ **Native Crash in 8.0 version on Nexus 6p device**   +1 ² | Hotlists (1) | Mark as Duplicate | 🔔 ⋮

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

[Infeasible]   Bug   P2 | + Add Hotlist

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

📄 **DESCRIPTION** ki...@gmail.com created issue #1   Nov 2, 2017 12:18AM   ⋮

Hi,

We are facing a crash issue in our application, with the following crash log in 8.0 version on Nexus 6p

App Description:
On launch of our application, we have v8 java script engine which will process the javascript input and show the UI.

Scenario:
The issue is happening some times , when a rendered map widget is removed from the layout
and the 'garbage collection' is triggered in both v8 Java Script Engine and Java layer.

NDK Version: 'android-ndk-r9d'
compile SDK Version: 15
target SDK Version: 15

Stacktrace:

10-26 08:22:50.584: A/RefBase(13403): decStrong() called on 0xd4236600 too many times
10-26 08:22:50.584: A/RefBase(13403): --------- beginning of crash
10-26 08:22:50.585: A/libc(13403): Fatal signal 6 (SIGABRT), code -6 in tid 13414 (FinalizerDaemon)
10-26 08:22:50.671: W/crash_dump32(13832): type=1400 audit(0.0:240): avc: denied { search } for
name="com.orgname.QNBProj" dev="dm-2" ino=1688761 scontext=u:r:crash_dump:s0:c512,c768
tcontext=u:object_r:app_data_file:s0:c512,c768 tclass=dir permissive=0
10-26 08:22:50.693: I/crash_dump32(13832): obtaining output fd from tombstoned
10-26 08:22:50.694: I//system/bin/tombstoned(597): received crash request for pid 13403
10-26 08:22:50.705: I/crash_dump32(13832): performing dump of process 13403 (target tid = 13414)
10-26 08:22:50.706: A/DEBUG(13832): *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
10-26 08:22:50.706: A/DEBUG(13832): Build fingerprint:
'google/angler/angler:8.0.0/OPR5.170623.007/4302479:user/release-keys'
10-26 08:22:50.706: A/DEBUG(13832): Revision: '0'
10-26 08:22:50.706: A/DEBUG(13832): ABI: 'arm'
10-26 08:22:50.706: A/DEBUG(13832): pid: 13403, tid: 13414, name: FinalizerDaemon >>>
com.orgname.QNBProj <<<
10-26 08:22:50.706: A/DEBUG(13832): signal 6 (SIGABRT), code -6 (SI_TKILL), fault addr --------
10-26 08:22:50.710: A/DEBUG(13832): Abort message: 'decStrong() called on 0xd4236600 too many times'
10-26 08:22:50.710: A/DEBUG(13832):   r0 00000000 r1 00003466 r2 00000006 r3 00000008
10-26 08:22:50.710: A/DEBUG(13832):   r4 0000345b r5 00003466 r6 d8219660 r7 0000010c
10-26 08:22:50.710: A/DEBUG(13832):   r8 f357be68 r9 bf605d00 sl d8219bd0 fp d8219b5c
10-26 08:22:50.710: A/DEBUG(13832):   ip 00000000 sp d8219650 lr f46ed3b7 pc f471d91c cpsr 200e0010
10-26 08:22:51.017: A/DEBUG(13832): backtrace:
10-26 08:22:51.017: A/DEBUG(13832):   #00 pc 0004a91c /system/lib/libc.so (tgkill+12)
10-26 08:22:51.017: A/DEBUG(13832):   #01 pc 0001a3b3 /system/lib/libc.so (abort+54)
10-26 08:22:51.017: A/DEBUG(13832):   #02 pc 000065f9 /system/lib/liblog.so (__android_log_assert+152)
10-26 08:22:51.017: A/DEBUG(13832):   #03 pc 0000adbb /system/lib/libutils.so
(_ZNK7android7RefBase9decStrongEPKv+94)
10-26 08:22:51.017: A/DEBUG(13832):   #04 pc 000c1043 /system/lib/libandroid_runtime.so
(_ZL30android_os_BinderProxy_destroyP7_JNIEnvP8_jobject+130)
10-26 08:22:51.017: A/DEBUG(13832):   #05 pc 005bb6d3 /system/framework/arm/boot-framework.oat
(offset 0x5bb000) (android.os.Binder.destroy [DEDUPED]+74)
10-26 08:22:51.017: A/DEBUG(13832):   #06 pc 003dc1e1 /system/lib/libart.so
(art_quick_invoke_stub_internal+64)
10-26 08:22:51.017: A/DEBUG(13832):   #07 pc 003e0755 /system/lib/libart.so (art_quick_invoke_stub+228)
10-26 08:22:51.017: A/DEBUG(13832):   #08 pc 000ac2ed /system/lib/libart.so
(_ZN3art9ArtMethod6InvokeEPNS_6ThreadEPjjPNS_6JValueEPKc+140)
10-26 08:22:51.017: A/DEBUG(13832):   #09 pc 001f16df /system/lib/libart.so
(_ZN3art11interpreter34ArtInterpreterToCompiledCodeBridgeEPNS_6ThreadEPNS_9ArtMethodEPKNS_7DexFile
8CodeItemEPNS_11ShadowFrameEPNS_6JValueE+238)
10-26 08:22:51.017: A/DEBUG(13832):   #10 pc 001ecc8f /system/lib/libart.so

---

Reporter   ⬤ ki...@gmail.com

Type   Bug

Priority   P2

Severity   S2

Status   [Won't fix (Infeasible)]

Access   Default access   View

Assignee   ⬤ ar...@google.com

Verifier   --

Collaborators   👥 _____ ⌃

CC   �öü _____ ⌃
ar...@google.com
ki...@gmail.com

AOSP ID   --

ReportedBy   --

Found In   --

Targeted To   --

Verified In   --

In Prod   ◯

(_ZN3art11interpreter6DoCallILb0ELb0EEEbPNS_9ArtMethodEPNS_6ThreadERNS_11ShadowFrameEPKNS_11InstructionEtPNS_6JValueE+574)
10-26 08:22:51.017: A/DEBUG(13832):   #11 pc 003c6f71 /system/lib/libart.so (MterpInvokeDirect+360)
10-26 08:22:51.017: A/DEBUG(13832):   #12 pc 003ce594 /system/lib/libart.so (ExecuteMterpImpl+14484)
10-26 08:22:51.017: A/DEBUG(13832):   #13 pc 001d4211 /system/lib/libart.so
(_ZN3art11interpreterL7ExecuteEPNS_6ThreadEPKNS_7DexFile8CodeItemERNS_11ShadowFrameENS_6JValueEb+340)
10-26 08:22:51.017: A/DEBUG(13832):   #14 pc 001d9593 /system/lib/libart.so
(_ZN3art11interpreter33ArtInterpreterToInterpreterBridgeEPNS_6ThreadEPKNS_7DexFile8CodeItemEPNS_11ShadowFrameEPNS_6JValueE+142)
10-26 08:22:51.017: A/DEBUG(13832):   #15 pc 001ecc79 /system/lib/libart.so
(_ZN3art11interpreter6DoCallILb0ELb0EEEbPNS_9ArtMethodEPNS_6ThreadERNS_11ShadowFrameEPKNS_11InstructionEtPNS_6JValueE+552)
10-26 08:22:51.017: A/DEBUG(13832):   #16 pc 003c60bb /system/lib/libart.so (MterpInvokeVirtual+446)
10-26 08:22:51.017: A/DEBUG(13832):   #17 pc 003ce494 /system/lib/libart.so (ExecuteMterpImpl+14228)
10-26 08:22:51.017: A/DEBUG(13832):   #18 pc 001d4211 /system/lib/libart.so
(_ZN3art11interpreterL7ExecuteEPNS_6ThreadEPKNS_7DexFile8CodeItemERNS_11ShadowFrameENS_6JValueEb+340)
10-26 08:22:51.017: A/DEBUG(13832):   #19 pc 001d9593 /system/lib/libart.so
(_ZN3art11interpreter33ArtInterpreterToInterpreterBridgeEPNS_6ThreadEPKNS_7DexFile8CodeItemEPNS_11ShadowFrameEPNS_6JValueE+142)
10-26 08:22:51.017: A/DEBUG(13832):   #20 pc 001ecc79 /system/lib/libart.so
(_ZN3art11interpreter6DoCallILb0ELb0EEEbPNS_9ArtMethodEPNS_6ThreadERNS_11ShadowFrameEPKNS_11InstructionEtPNS_6JValueE+552)
10-26 08:22:51.017: A/DEBUG(13832):   #21 pc 003c6f71 /system/lib/libart.so (MterpInvokeDirect+360)
10-26 08:22:51.017: A/DEBUG(13832):   #22 pc 003ce594 /system/lib/libart.so (ExecuteMterpImpl+14484)
10-26 08:22:51.017: A/DEBUG(13832):   #23 pc 001d4211 /system/lib/libart.so
(_ZN3art11interpreterL7ExecuteEPNS_6ThreadEPKNS_7DexFile8CodeItemERNS_11ShadowFrameENS_6JValueEb+340)
10-26 08:22:51.017: A/DEBUG(13832):   #24 pc 001d9593 /system/lib/libart.so
(_ZN3art11interpreter33ArtInterpreterToInterpreterBridgeEPNS_6ThreadEPKNS_7DexFile8CodeItemEPNS_11ShadowFrameEPNS_6JValueE+142)
10-26 08:22:51.017: A/DEBUG(13832):   #25 pc 001ecc79 /system/lib/libart.so
(_ZN3art11interpreter6DoCallILb0ELb0EEEbPNS_9ArtMethodEPNS_6ThreadERNS_11ShadowFrameEPKNS_11InstructionEtPNS_6JValueE+552)
10-26 08:22:51.017: A/DEBUG(13832):   #26 pc 003c60bb /system/lib/libart.so (MterpInvokeVirtual+446)
10-26 08:22:51.017: A/DEBUG(13832):   #27 pc 003ce494 /system/lib/libart.so (ExecuteMterpImpl+14228)
10-26 08:22:51.017: A/DEBUG(13832):   #28 pc 001d4211 /system/lib/libart.so
(_ZN3art11interpreterL7ExecuteEPNS_6ThreadEPKNS_7DexFile8CodeItemERNS_11ShadowFrameENS_6JValueEb+340)
10-26 08:22:51.017: A/DEBUG(13832):   #29 pc 001d9593 /system/lib/libart.so
(_ZN3art11interpreter33ArtInterpreterToInterpreterBridgeEPNS_6ThreadEPKNS_7DexFile8CodeItemEPNS_11ShadowFrameEPNS_6JValueE+142)
10-26 08:22:51.017: A/DEBUG(13832):   #30 pc 001ecc79 /system/lib/libart.so
(_ZN3art11interpreter6DoCallILb0ELb0EEEbPNS_9ArtMethodEPNS_6ThreadERNS_11ShadowFrameEPKNS_11InstructionEtPNS_6JValueE+552)
10-26 08:22:51.017: A/DEBUG(13832):   #31 pc 003c6ce7 /system/lib/libart.so (MterpInvokeInterface+1198)
10-26 08:22:51.017: A/DEBUG(13832):   #32 pc 003ce694 /system/lib/libart.so (ExecuteMterpImpl+14740)
10-26 08:22:51.017: A/DEBUG(13832):   #33 pc 001d4211 /system/lib/libart.so
(_ZN3art11interpreterL7ExecuteEPNS_6ThreadEPKNS_7DexFile8CodeItemERNS_11ShadowFrameENS_6JValueEb+340)
10-26 08:22:51.017: A/DEBUG(13832):   #34 pc 001d94e1 /system/lib/libart.so
(_ZN3art11interpreter30EnterInterpreterFromEntryPointEPNS_6ThreadEPKNS_7DexFile8CodeItemEPNS_11ShadowFrameE+92)
10-26 08:22:51.017: A/DEBUG(13832):   #35 pc 003bc7f5 /system/lib/libart.so
(artQuickToInterpreterBridge+960)
10-26 08:22:51.017: A/DEBUG(13832):   #36 pc 003dffa1 /system/lib/libart.so
(art_quick_to_interpreter_bridge+32)
10-26 08:22:51.017: A/DEBUG(13832):   #37 pc 003dc1e1 /system/lib/libart.so
(art_quick_invoke_stub_internal+64)
10-26 08:22:51.017: A/DEBUG(13832):   #38 pc 003e0755 /system/lib/libart.so (art_quick_invoke_stub+228)
10-26 08:22:51.017: A/DEBUG(13832):   #39 pc 000ac2ed /system/lib/libart.so
(_ZN3art9ArtMethod6InvokeEPNS_6ThreadEPjjPNS_6JValueEPKc+140)
10-26 08:22:51.017: A/DEBUG(13832):   #40 pc 003319cd /system/lib/libart.so
(_ZN3artL18InvokeWithArgArrayERKNS_33ScopedObjectAccessAlreadyRunnableEPNS_9ArtMethodEPNS_8ArgArrayEPNS_6JValueEPKc+52)
10-26 08:22:51.017: A/DEBUG(13832):   #41 pc 00332841 /system/lib/libart.so
(_ZN3art35InvokeVirtualOrInterfaceWithJValuesERKNS_33ScopedObjectAccessAlreadyRunnableEP8_jobjectP10_jmethodIDP6jvalue+320)
10-26 08:22:51.017: A/DEBUG(13832):   #42 pc 003500b1 /system/lib/libart.so
(_ZN3art6Thread14CreateCallbackEPv+892)
10-26 08:22:51.017: A/DEBUG(13832):   #43 pc 00047c3f /system/lib/libc.so (_ZL15__pthread_startPv+22)
10-26 08:22:51.017: A/DEBUG(13832):   #44 pc 0001af5d /system/lib/libc.so (__start_thread+32)
10-26 08:22:52.283: E//system/bin/tombstoned(597): Tombstone written to: /data/tombstones//tombstone_05
10-26 08:22:52.296: I/BootReceiver(782): Copying /data/tombstones/tombstone_05 to DropBox
(SYSTEM_TOMBSTONE)
10-26 08:22:52.301: W/ActivityManager(782):   Force finishing activity com.orgname.QNBProj/.QNB

10-26 08:22:52.323: I/ActivityManager(782): Showing crash dialog for package com.orgname.QNBProj u0
10-26 08:22:52.325: E/lowmemorykiller(426): Error writing /proc/13403/oom_score_adj; errno=22
10-26 08:22:52.394: I/ActivityManager(782): Process com.orgname.QNBProj (pid 13403) has died: vis +99TOP
10-26 08:22:52.396: I/OpenGLRenderer(782): Initialized EGL, version 1.4
10-26 08:22:52.396: D/OpenGLRenderer(782): Swap behavior 2
10-26 08:22:52.397: I/WindowManager(782): WIN DEATH: Window{db25245 u0
com.orgname.QNBProj/com.orgname.QNBProj.QNB}
10-26 08:22:52.401: I/Zygote(574): Process 13403 exited due to signal (6)
10-26 08:22:52.411: W/ActivityManager(782): setHasOverlayUi called on unknown pid: 13403
10-26 08:22:52.563: W/Looper(782): Dispatch took 154ms on android.ui, h=Handler
(android.view.Choreographer$FrameHandler) {f1e339c}
cb=android.view.Choreographer$FrameDisplayEventReceiver@a3db1a5 msg=0
10-26 08:22:52.982: E/QC-QMI(564): linux_qmi_qmux_io_wake_lock: Err in writing wakelock=qmuxd_port_wl_0,
error [1:Operation not permitted]
10-26 08:22:52.983: E/QC-QMI(564): linux_qmi_qmux_io_wake_unlock: Err in writing
wakelock=qmuxd_port_wl_0, error [1:Operation not permitted]
10-26 08:22:58.109: E/QC-QMI(564): linux_qmi_qmux_io_wake_lock: Err in writing wakelock=qmuxd_port_wl_0,
error [1:Operation not permitted]
10-26 08:22:58.109: E/QC-QMI(564): linux_qmi_qmux_io_wake_unlock: Err in writing
wakelock=qmuxd_port_wl_0, error [1:Operation not permitted]
10-26 08:23:00.670: E/QC-QMI(564): linux_qmi_qmux_io_wake_lock: Err in writing wakelock=qmuxd_port_wl_0,
error [1:Operation not permitted]
10-26 08:23:00.670: E/QC-QMI(564): linux_qmi_qmux_io_wake_unlock: Err in writing
wakelock=qmuxd_port_wl_0, error [1:Operation not permitted]
10-26 08:23:00.784: W/ActivityManager(782): Ignoring remove of inactive process: ProcessRecord{a8c480a
0:com.orgname.QNBProj/u0a120}
10-26 08:23:00.785: I/ActivityManager(782): START u0 {act=android.intent.action.MAIN cat=
[android.intent.category.LAUNCHER] flg=0x10300000 cmp=com.orgname.QNBProj/.QNB bnds=[113,378]
[337,602] (has extras)} from uid 10040
10-26 08:23:00.813: E/ActivityManager(782): applyOptionsLocked: Unknown animationType=0
10-26 08:23:00.830: I/ActivityManager(782): Start proc 13847:com.orgname.QNBProj/u0a120 for activity
com.orgname.QNBProj/.QNB
10-26 08:23:00.830: I/zygote(13847): Late-enabling -Xcheck:jni
10-26 08:23:00.892: E/zygote(13847): Failed sending reply to debugger: Broken pipe
10-26 08:23:00.892: I/zygote(13847): Debugger is no longer active
10-26 08:23:00.967: D/KonyMain(13847): OnCreate
10-26 08:23:01.011: W/AppOps(782): Finishing op nesting under-run: uid 1000 pkg android code 24 time=0
duration=0 nesting=0
10-26 08:23:01.201: D/KonyMain(13847): splash image file name is :::::splash.9.png
10-26 08:23:01.203: D/KonySkin(13847): Application Memory : 192MB
10-26 08:23:01.205: D/KonySkin(13847): Limiting bitmap cache size to : 24.0MB
10-26 08:23:01.209: D/KonyMain(13847): The Image file drawbale is splash
10-26 08:23:01.285: I/InputDispatcher(782): Dropping event because there is no touchable window at (0, 2305).
: E/(): Device disconnected

Please let us know if this is a native android OS libart crash happening because of an issue in ART
implementation .
If not can you throw us a light as to when this can occur if you think it is an application issue, as same apk is
working fine in other OS versions.

Additionally this is happening only on Nexus 6p with 8.0 os and is not replicable always.

And Can this happen because of older NDK version 'android-ndk-r9d'?

Thanks,
Kiran

COMMENTS   All comments   ▼   ↓ Oldest first

⬤   **ar...@google.com** <ar...@google.com> #2   Nov 3, 2017 10:53PM   ⋮

     Assigned to ar...@google.com.

     Thank you for reporting this issue. For us to further investigate this issue, please provide the following
     additional information:

     Steps to reproduce
     What steps are needed to reproduce this issue?

     Frequency
     How frequently does this issue occur? (e.g 100% of the time, 10% of the time)

     Expected output
     What is the expected output?

     Current output

What is the current output?

Android bug report
After reproducing the issue, press the volume up, volume down, and power button simultaneously. This will capture a bug report on your device in the "bug reports" directory. Attach the bug report file to this issue.

Alternate method:
After reproducing the issue, navigate to developer settings, ensure 'USB debugging' is enabled, then enable 'Bug report shortcut'. To take bug report, hold the power button and select the 'Take bug report' option.

○ **ar...@google.com** <ar...@google.com> #3   Dec 19, 2017 02:32AM ⋮

Status: Won't Fix (Infeasible)

We are closing this issue as we don't have enough actionable information. If you are still facing this problem, please open new issue and add the relevant information along with reference to earlier issue.