



Comments (6) Dependencies Duplicates (0) Blocking (0) Resources (1)

Can't Repro Bug P2 + Add Hotlist [AOSP] assigned

STATUS UPDATE No update yet. Edit

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

creating an encoder (using e.g `MediaCodec.createEncoderByType("video/avc")`) and releasing it multiple times causes a weak global reference table overflow. The reported bug can simply be reproduced running the following lines of code (in an app that does nothing else)

```
for(int i=0;i<53000;i++)
{
```

```
    MediaCodec C = null;
    try
    {
        C = MediaCodec.createEncoderByType("video/avc");
    }catch(Exception e)
    {

    }

    C.stop();
    C.release();

}
```

I have seen that bug on different mobile phones, e.g Google Pixel 2 (Android 8.1.0, Android security patch level May 5, 2018, Build Number OPM2.171019.029.B1)

10-08 03:08:32.535 5166-3699/com.xxx.st.vs.test.test I/OMXClient: Treble IOmx obtained
10-08 03:08:32.581 5166-3706/com.xxx.st.vs.test.test I/OMXClient: Treble IOmx obtained
10-08 03:08:32.636 5166-5166/com.xxx.st.vs.test.test A/zygote64: indirect_reference_table.cc:256] JNI ERROR (app bug): weak global reference table overflow (max=51200)
indirect_reference_table.cc:256] weak global reference table dump:
indirect_reference_table.cc:256] Last 10 entries (of 51199):
indirect_reference_table.cc:256] 51198: 0x12ec0028 java.lang.Thread
indirect_reference_table.cc:256] 51197: 0x12e80028 java.lang.Thread
indirect_reference_table.cc:256] 51196: 0x12e40028 java.lang.Thread
indirect_reference_table.cc:256] 51195: 0x12e00028 java.lang.Thread
indirect_reference_table.cc:256] 51194: 0x12dc0028 java.lang.Thread
indirect_reference_table.cc:256] 51193: 0x12d80028 java.lang.Thread
indirect_reference_table.cc:256] 51192: 0x12d40028 java.lang.Thread
indirect_reference_table.cc:256] 51191: 0x12d00028 java.lang.Thread
indirect_reference_table.cc:256] 51190: 0x12cc0028 java.lang.Thread
indirect_reference_table.cc:256] 51189: 0x12c80028 java.lang.Thread
indirect_reference_table.cc:256] Summary:
indirect_reference_table.cc:256] 5195 of java.lang.Class (5195 unique instances)
indirect_reference_table.cc:256] 18 of java.lang.Thread (18 unique instances)
indirect_reference_table.cc:256] 18 of java.lang.DexCache (18 unique instances)
indirect_reference_table.cc:256] 3 of dalvik.system.PathClassLoader (2 unique instances)
indirect_reference_table.cc:256] 3 of java.lang.String (3 unique instances)
indirect_reference_table.cc:256] 2 of java.lang.ThreadGroup (2 unique instances)
indirect_reference_table.cc:256] 1 of com.xxx.st.vs.test.test.MainActivity
indirect_reference_table.cc:256] 1 of android.support.v7.app.AppCompatActivity
10-08 03:08:32.637 5166-5166/com.xxx.st.vs.test.test A/zygote64: indirect_reference_table.cc:256] 1 of android.arch.lifecycle.LifecycleRegistry
indirect_reference_table.cc:256] 1 of android.support.v4.app.FragmentActivity\$1
indirect_reference_table.cc:256] 1 of android.support.v4.app.FragmentController
indirect_reference_table.cc:256] 1 of android.support.v4.util.SparseArrayCompat
indirect_reference_table.cc:256] 1 of android.support.v4.util.SimpleArrayMap
indirect_reference_table.cc:256] 1 of java.lang.BootClassLoader
indirect_reference_table.cc:256] 1 of java.util.ArrayList
indirect_reference_table.cc:256] 1 of android.app.ContextImpl
indirect_reference_table.cc:256] 1 of android.app.ActivityThread
indirect_reference_table.cc:256] 1 of android.os.Handler
indirect_reference_table.cc:256] 1 of com.android.internal.policy.PhoneWindow
indirect_reference_table.cc:256] 1 of android.content.pm.ActivityInfo
indirect_reference_table.cc:256] 1 of android.content.res.Resources
indirect_reference_table.cc:256] 1 of android.app.ActivityThread\$H
indirect_reference_table.cc:256] 1 of android.content.res.Resources\$Theme
indirect_reference_table.cc:256] 1 of android.os.StrictMode\$InstanceTracker
indirect_reference_table.cc:256] 1 of android.content.ComponentName
indirect_reference_table.cc:256] 1 of android.app.Application
indirect_reference_table.cc:256] 1 of android.app.ActivityManager\$TaskDescription
indirect_reference_table.cc:256] 1 of android.view.WindowManagerImpl
indirect_reference_table.cc:256] 1 of android.app.SharedElementCallback\$1
indirect_reference_table.cc:256] 1 of android.os.BinderProxy

```
indirect_reference_table.cc:256] 1 of android.content.res.Configuration
indirect_reference_table.cc:256] 1 of android.app.Instrumentation
indirect_reference_table.cc:256] 1 of android.content.Intent
indirect_reference_table.cc:256] 1 of android.app.ActivityTransitionState
indirect_reference_table.cc:256] 1 of com.android.internal.policy.PhoneLayoutInflater
indirect_reference_table.cc:256] 1 of com.android.internal.os.RuntimeInit$MethodAndArgsCaller
indirect_reference_table.cc:256] 1 of android.app.FragmentController
indirect_reference_table.cc:256]
10-08 03:08:32.706 5166-5166/com.xxx.st.vstest.test A/zygote64: runtime.cc:523] Runtime aborting...
runtime.cc:523] Dumping all threads without appropriate locks held: thread list lock
runtime.cc:523] All threads:
runtime.cc:523] DALVIK THREADS (13):
runtime.cc:523] "main" prio=10 tid=1 Runnable
runtime.cc:523] | group="" sCount=0 dsCount=0 flags=0 obj=0x728ec610 self=0x77d5e000
runtime.cc:523] | sysTid=5166 nice=-10 cgrp=default sched=0/0 handle=0x785a9a8
runtime.cc:523] | state=R schedstat=( 115837340364 37307193313 565330 ) utm=7012 stm=4571 core=4 HZ=100
runtime.cc:523] | stack=0x7ffb5d5000-0x7ffb5d7000 stackSize=8MB
runtime.cc:523] | held mutexes= "abort lock" "JNI weak global reference table lock" "mutator lock"(shared held)
runtime.cc:523] native: #00 pc 00000000003ccb5c /system/lib64/libart.so (art::DumpNativeStack(std::__1::basic_ostream<char, std::__1::char_traits<char>>&, int, BacktraceMap*, char const
runtime.cc:523] native: #01 pc 000000000049cdf4 /system/lib64/libart.so (art::Thread::DumpStack(std::__1::basic_ostream<char, std::__1::char_traits<char>>&, bool, BacktraceMap*, bool) cc
runtime.cc:523] native: #02 pc 00000000004b4b68 /system/lib64/libart.so (art::DumpCheckpoint::Run(art::Thread*)+884)
runtime.cc:523] native: #03 pc 00000000004ad374 /system/lib64/libart.so (art::ThreadList::RunCheckpoint(art::Closure*, art::Closure*)+472)
runtime.cc:523] native: #04 pc 00000000004acaf8 /system/lib64/libart.so (art::ThreadList::Dump(std::__1::basic_ostream<char, std::__1::char_traits<char>>&, bool)+288)
runtime.cc:523] native: #05 pc 000000000048435c /system/lib64/libart.so (art::AbortState::Dump(std::__1::basic_ostream<char, std::__1::char_traits<char>>&) const+220)
runtime.cc:523] native: #06 pc 000000000047598c /system/lib64/libart.so (art::Runtime::Abort(char const*)+196)
runtime.cc:523] native: #07 pc 000000000056b3ec /system/lib64/libart.so (android::base::LogMessage::~~LogMessage()+1004)
runtime.cc:523] native: #08 pc 0000000000263778 /system/lib64/libart.so (art::IndirectReferenceTable::Add(art::IRTSegmentState, art::ObjPtr<art::mirror::Object>)+764)
runtime.cc:523] native: #09 pc 00000000002fecdc /system/lib64/libart.so (art::JavaVMExt::AddWeakGlobalRef(art::Thread*, art::ObjPtr<art::mirror::Object>)+68)
runtime.cc:523] native: #10 pc 0000000000385100 /system/lib64/libart.so (art::JNI::NewWeakGlobalRef(_JNIEnv*, _jobject*)+572)
runtime.cc:523] native: #11 pc 000000000010eb80 /system/lib64/libart.so (art::CheckJNI::NewRef(char const*, _JNIEnv*, _jobject*, art::IndirectRefKind)+704)
runtime.cc:523] native: #12 pc 000000000002b220 /system/lib64/libmedia_jni.so (android::JMediaCodec::JMediaCodec(_JNIEnv*, _jobject*, char const*, bool, bool)+248)
runtime.cc:523] native: #13 pc 0000000000030800 /system/lib64/libmedia_jni.so (???)
runtime.cc:523] native: #14 pc 00000000007123c8 /system/framework/arm64/boot-framework.oat (Java_android_media_MediaCodec_native_1setup__Ljava_lang_String_2ZZ+168)
runtime.cc:523] at android.media.MediaCodec.native_setup(Native method)
runtime.cc:523] at android.media.MediaCodec.<init>(MediaCodec.java:1794)
runtime.cc:523] at android.media.MediaCodec.createEncoderByType(MediaCodec.java:1760)
runtime.cc:523] at com.xxx.st.vstest.test.MainActivity.onCreate(MainActivity.java:23)
runtime.cc:523] at android.app.Activity.performCreate(Activity.java:6999)
runtime.cc:523] at android.app.Activity.performCreate(Activity.java:6990)
runtime.cc:523] at android.app.Instrumentation.callActivityOnCreate(Instrumentation.java:1214)
runtime.cc:523] at android.app.ActivityThread.performLaunchActivity(ActivityThread.java:2731)
runtime.cc:523] at android.app.ActivityThread.handleLaunchActivity(ActivityThread.java:2856)
runtime.cc:523] at android.app.ActivityThread.-wrap11(ActivityThread.java:-1)
runtime.cc:523] at android.app.ActivityThread$H.handleMessage(ActivityThread.java:1589)
runtime.cc:523] at android.os.Handler.dispatchMessage(Handler.java:106)
runtime.cc:523] at android.os.Looper.loop(Looper.java:164)
runtime.cc:523] at android.app.ActivityThread.main(ActivityThread.java:6494)
runtime.cc:523] at java.lang.reflect.Method.invoke(Native method)
runtime.cc:523] at com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run(RuntimeInit.java:438)
runtime.cc:523] at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:807)
runtime.cc:523]
runtime.cc:523] "Jit thread pool worker thread 0" prio=10 tid=2 Native
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x13840000 self=0x77cd80e000
runtime.cc:523] | sysTid=5173 nice=9 cgrp=default sched=0/0 handle=0x77cdd874f0
runtime.cc:523] | state=S schedstat=( 119242026 8253282 327 ) utm=8 stm=2 core=5 HZ=100
runtime.cc:523] | stack=0x77cdc89000-0x77cdc8b000 stackSize=1021KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: futex_wait_queue_me+0xc4/0x12c
runtime.cc:523] kernel: futex_wait+0xe8/0x2d0
runtime.cc:523] kernel: do_futex+0xf8/0x1408
runtime.cc:523] kernel: Sys_futex+0x144/0x19c
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 00000000001d4ac /system/lib64/libc.so (syscall+28)
runtime.cc:523] native: #01 pc 0000000000e663c /system/lib64/libart.so (art::ConditionVariable::WaitHoldingLocks(art::Thread*)+152)
runtime.cc:523] native: #02 pc 00000000004b6324 /system/lib64/libart.so (art::ThreadPool::GetTask(art::Thread*)+256)
runtime.cc:523] native: #03 pc 00000000004b5a18 /system/lib64/libart.so (art::ThreadPoolWorker::Run()+124)
10-08 03:08:32.707 5166-5166/com.xxx.st.vstest.test A/zygote64: runtime.cc:523] native: #04 pc 00000000004b54ec /system/lib64/libart.so (art::ThreadPoolWorker::Callback(void*)+148)
runtime.cc:523] native: #05 pc 000000000067d80 /system/lib64/libc.so (__pthread_start(void*)+36)
runtime.cc:523] native: #06 pc 00000000001ec18 /system/lib64/libc.so (__start_thread+68)
runtime.cc:523] (no managed stack frames)
runtime.cc:523]
runtime.cc:523] "Signal Catcher" prio=10 tid=3 WaitingInMainSignalCatcherLoop
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x13840088 self=0x77d5ebf400
runtime.cc:523] | sysTid=5174 nice=0 cgrp=default sched=0/0 handle=0x77cdc864f0
runtime.cc:523] | state=S schedstat=( 120157 8489 1 ) utm=0 stm=0 core=7 HZ=100
runtime.cc:523] | stack=0x77cdb8c000-0x77cdb8e000 stackSize=1005KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: do_sigtimedwait+0x148/0x324
runtime.cc:523] kernel: Sys_rt_sigtimedwait+0xf0/0x150
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000006a64c /system/lib64/libc.so (__rt_sigtimedwait+8)
runtime.cc:523] native: #01 pc 0000000000284dc /system/lib64/libc.so (sigwait+60)
runtime.cc:523] native: #02 pc 000000000048ba54 /system/lib64/libart.so (art::SignalSet::Wait()+44)
runtime.cc:523] native: #03 pc 000000000048b54c /system/lib64/libart.so (art::SignalCatcher::WaitForSignal(art::Thread*, art::SignalSet&)+252)
```

```
runtime.cc:523] native: #00 pc 0000000000489d28 /system/lib64/libart.so (art::SignalCatcher::Run(void*)+268)
runtime.cc:523] native: #05 pc 0000000000067d80 /system/lib64/libc.so (pthread_start(void*)+36)
runtime.cc:523] native: #06 pc 000000000001ec18 /system/lib64/libc.so (__start_thread+68)
runtime.cc:523] (no managed stack frames)
runtime.cc:523]
runtime.cc:523] "JDWP" prio=10 tid=4 WaitingInMainDebuggerLoop
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x13840110 self=0x77cd814400
runtime.cc:523] | sysTid=5175 nice=0 cgrp=default sched=0/0 handle=0x77c18f64f0
runtime.cc:523] | state=S schedstat=( 195399120 80425610 1444 ) utm=11 stm=7 core=5 HZ=100
runtime.cc:523] | stack=0x77c17fc000-0x77c17fe000 stackSize=1005KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: do_select+0x374/0x614
runtime.cc:523] kernel: core_sys_select+0x22c/0x370
runtime.cc:523] kernel: SyS_pselect6+0x304/0x378
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000006a5a4 /system/lib64/libc.so (__pselect6+8)
runtime.cc:523] native: #01 pc 00000000000265e8 /system/lib64/libc.so (select+144)
runtime.cc:523] native: #02 pc 00000000005584d0 /system/lib64/libart.so (art::JDWP::JdwpAdbState::ProcessIncoming()+336)
runtime.cc:523] native: #03 pc 0000000000312d90 /system/lib64/libart.so (art::JDWP::JdwpState::Run()+448)
runtime.cc:523] native: #04 pc 0000000000312464 /system/lib64/libart.so (art::JDWP::StartJdwpThread(void*)+40)
runtime.cc:523] native: #05 pc 0000000000067d80 /system/lib64/libc.so (pthread_start(void*)+36)
runtime.cc:523] native: #06 pc 000000000001ec18 /system/lib64/libc.so (__start_thread+68)
runtime.cc:523] (no managed stack frames)
runtime.cc:523]
runtime.cc:523] "FinalizerDaemon" prio=10 tid=5 Waiting
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x13840198 self=0x77d5ec1200
runtime.cc:523] | sysTid=5177 nice=4 cgrp=default sched=0/0 handle=0x77c16f44f0
runtime.cc:523] | state=S schedstat=( 772241191 27944642 840 ) utm=74 stm=2 core=4 HZ=100
runtime.cc:523] | stack=0x77c15f2000-0x77c15f4000 stackSize=1037KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: futex_wait_queue_me+0xc4/0x12c
runtime.cc:523] kernel: futex_wait+0xe8/0x2d0
runtime.cc:523] kernel: do_futex+0xf8/0x1408
runtime.cc:523] kernel: SyS_futex+0x144/0x19c
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000001d4ac /system/lib64/libc.so (syscall+28)
runtime.cc:523] native: #01 pc 00000000000e663c /system/lib64/libart.so (art::ConditionVariable::WaitHoldingLocks(art::Thread*)+152)
runtime.cc:523] native: #02 pc 00000000003c7dd4 /system/lib64/libart.so (art::Monitor::Wait(art::Thread*, long, int, bool, art::ThreadState)+636)
runtime.cc:523] native: #03 pc 00000000003c9864 /system/lib64/libart.so (art::Monitor::Wait(art::Thread*, long, int, bool, art::ThreadState)+376)
runtime.cc:523] native: #04 pc 0000000000000aec /system/framework/arm64/boot.oat (Java_java_lang_Object_wait__JI+140)
runtime.cc:523] at java.lang.Object.wait(Native method)
runtime.cc:523] - waiting on <0x00c1748f> (a java.lang.Object)
runtime.cc:523] at java.lang.Object.wait(Object.java:422)
runtime.cc:523] at java.lang.ref.ReferenceQueue.remove(ReferenceQueue.java:188)
runtime.cc:523] - locked <0x00c1748f> (a java.lang.Object)
runtime.cc:523] at java.lang.ref.ReferenceQueue.remove(ReferenceQueue.java:209)
runtime.cc:523] at java.lang.Daemons$FinalizerDaemon.runInternal(Daemons.java:232)
runtime.cc:523] at java.lang.Daemons$Daemon.run(Daemons.java:103)
runtime.cc:523] at java.lang.Thread.run(Thread.java:764)
runtime.cc:523]
runtime.cc:523] "FinalizerWatchdogDaemon" prio=10 tid=6 Sleeping
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x13840220 self=0x77d5ed4400
runtime.cc:523] | sysTid=5178 nice=4 cgrp=default sched=0/0 handle=0x77c15ef4f0
runtime.cc:523] | state=S schedstat=( 66264012 5253596 333 ) utm=5 stm=0 core=5 HZ=100
runtime.cc:523] | stack=0x77c14ed000-0x77c14ef000 stackSize=1037KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: futex_wait_queue_me+0xc4/0x12c
runtime.cc:523] kernel: futex_wait+0xe8/0x2d0
runtime.cc:523] kernel: do_futex+0xf8/0x1408
runtime.cc:523] kernel: SyS_futex+0x144/0x19c
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000001d4b0 /system/lib64/libc.so (syscall+32)
runtime.cc:523] native: #01 pc 00000000000e6a5c /system/lib64/libart.so (art::ConditionVariable::TimedWait(art::Thread*, long, int)+172)
runtime.cc:523] native: #02 pc 00000000003c7de4 /system/lib64/libart.so (art::Monitor::Wait(art::Thread*, long, int, bool, art::ThreadState)+652)
runtime.cc:523] native: #03 pc 00000000003c9864 /system/lib64/libart.so (art::Monitor::Wait(art::Thread*, art::mirror::Object*, long, int, bool, art::ThreadState)+376)
runtime.cc:523] native: #04 pc 000000000001e3ec /system/framework/arm64/boot.oat (Java_java_lang_Thread_sleep__Ljava_lang_Object_2J+188)
runtime.cc:523] at java.lang.Thread.sleep(Native method)
runtime.cc:523] - sleeping on <0x097c631c> (a java.lang.Object)
runtime.cc:523] at java.lang.Thread.sleep(Thread.java:373)
runtime.cc:523] - locked <0x097c631c> (a java.lang.Object)
runtime.cc:523] at java.lang.Thread.sleep(Thread.java:314)
runtime.cc:523] at java.lang.Daemons$FinalizerWatchdogDaemon.sleepFor(Daemons.java:342)
runtime.cc:523] at java.lang.Daemons$FinalizerWatchdogDaemon.waitForFinalization(Daemons.java:364)
runtime.cc:523] at java.lang.Daemons$FinalizerWatchdogDaemon.runInternal(Daemons.java:281)
runtime.cc:523] at java.lang.Daemons$Daemon.run(Daemons.java:103)
runtime.cc:523] at java.lang.Thread.run(Thread.java:764)
runtime.cc:523]
runtime.cc:523] "HeapTaskDaemon" prio=10 tid=7 Blocked
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x138404c8 self=0x77d5ed4e00
runtime.cc:523] | sysTid=5179 nice=4 cgrp=default sched=0/0 handle=0x77c14ea4f0
runtime.cc:523] | state=S schedstat=( 8411886555 962613214 8594 ) utm=799 stm=41 core=4 HZ=100
runtime.cc:523] | stack=0x77c13e8000-0x77c13ea000 stackSize=1037KB
runtime.cc:523] | held mutexes=
```

```
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: futex_wait_queue_me+0xc4/0x12c
runtime.cc:523] kernel: futex_wait+0xe8/0x2d0
runtime.cc:523] kernel: do_futex+0xf8/0x1408
runtime.cc:523] kernel: SyS_futex+0x144/0x19c
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
10-08 03:08:32.708 5166-5166/com.xxx.st.vs.test.test A/zygote64: runtime.cc:523] native: #00 pc 000000000001d4b0 /system/lib64/libc.so (syscall+32)
runtime.cc:523] native: #01 pc 00000000000e6a5c /system/lib64/libart.so (art::ConditionVariable::TimedWait(art::Thread*, long, int)+172)
runtime.cc:523] native: #02 pc 0000000000253aac /system/lib64/libart.so (art::gc::TaskProcessor::GetTask(art::Thread*)+344)
runtime.cc:523] native: #03 pc 000000000025438c /system/lib64/libart.so (art::gc::TaskProcessor::RunAllTasks(art::Thread*)+92)
runtime.cc:523] native: #04 pc 00000000001f2f2c /system/framework/arm64/boot-core-libart.oat (Java_dalvik_system_VMRuntime_runHeapTasks__+124)
runtime.cc:523] at dalvik.system.VMRuntime.runHeapTasks(Native method)
runtime.cc:523] - waiting to lock an unknown object
runtime.cc:523] at java.lang.Daemons$HeapTaskDaemon.runInternal(Daemons.java:461)
runtime.cc:523] at java.lang.Daemons$Daemon.run(Daemons.java:103)
runtime.cc:523] at java.lang.Thread.run(Thread.java:764)
runtime.cc:523]
runtime.cc:523] "ReferenceQueueDaemon" prio=10 tid=8 Waiting
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x138402a8 self=0x77d5ec0800
runtime.cc:523] | sysTid=5176 nice=4 cgrp=default sched=0/0 handle=0x77c17f94f0
runtime.cc:523] | state=S schedstat=( 148442253 5929420 587 ) utm=9 stm=5 core=5 HZ=100
runtime.cc:523] | stack=0x77c16f7000-0x77c16f9000 stackSize=1037KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: futex_wait_queue_me+0xc4/0x12c
runtime.cc:523] kernel: futex_wait+0xe8/0x2d0
runtime.cc:523] kernel: do_futex+0xf8/0x1408
runtime.cc:523] kernel: SyS_futex+0x144/0x19c
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000001d4ac /system/lib64/libc.so (syscall+28)
runtime.cc:523] native: #01 pc 00000000000e663c /system/lib64/libart.so (art::ConditionVariable::WaitHoldingLocks(art::Thread*)+152)
runtime.cc:523] native: #02 pc 00000000003c7dd4 /system/lib64/libart.so (art::Monitor::Wait(art::Thread*, long, int, bool, art::ThreadState)+636)
runtime.cc:523] native: #03 pc 00000000003c9864 /system/lib64/libart.so (art::Monitor::Wait(art::Thread*, art::mirror::Object*, long, int, bool, art::ThreadState)+376)
runtime.cc:523] native: #04 pc 000000000000070c /system/framework/arm64/boot.oat (Java_java_lang_Object_wait__+124)
runtime.cc:523] at java.lang.Object.wait(Native method)
runtime.cc:523] - waiting on <0x096071ff> (a java.lang.Class<java.lang.ref.ReferenceQueue>)
runtime.cc:523] at java.lang.Daemons$ReferenceQueueDaemon.runInternal(Daemons.java:178)
runtime.cc:523] - locked <0x096071ff> (a java.lang.Class<java.lang.ref.ReferenceQueue>)
runtime.cc:523] at java.lang.Daemons$Daemon.run(Daemons.java:103)
runtime.cc:523] at java.lang.Thread.run(Thread.java:764)
runtime.cc:523]
runtime.cc:523] "Binder:5166_1" prio=10 tid=9 Native
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x13840330 self=0x77d5f99400
runtime.cc:523] | sysTid=5180 nice=0 cgrp=default sched=0/0 handle=0x77c12e74f0
runtime.cc:523] | state=S schedstat=( 4522745362 698936387 50083 ) utm=122 stm=329 core=4 HZ=100
runtime.cc:523] | stack=0x77c11ed000-0x77c11ef000 stackSize=1005KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: binder_ioctl_write_read+0x34dc/0x41d4
runtime.cc:523] kernel: binder_ioctl+0x2b4/0xa9c
runtime.cc:523] kernel: do_vfs_ioctl+0x434/0x884
runtime.cc:523] kernel: SyS_ioctl+0x88/0x94
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000006a558 /system/lib64/libc.so (__ioctl+4)
runtime.cc:523] native: #01 pc 0000000000023ebc /system/lib64/libc.so (ioctl+136)
runtime.cc:523] native: #02 pc 000000000054938 /system/lib64/libbinder.so (android::IPCThreadState::talkWithDriver(bool)+260)
runtime.cc:523] native: #03 pc 0000000000054aa8 /system/lib64/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+24)
runtime.cc:523] native: #04 pc 000000000005516c /system/lib64/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+60)
runtime.cc:523] native: #05 pc 000000000007615c /system/lib64/libbinder.so (???)
runtime.cc:523] native: #06 pc 000000000011478 /system/lib64/libutils.so (android::Thread::_threadLoop(void*)+280)
runtime.cc:523] native: #07 pc 00000000000a9814 /system/lib64/libandroid_runtime.so (android::AndroidRuntime::javaThreadShell(void*)+140)
runtime.cc:523] native: #08 pc 0000000000067d80 /system/lib64/libc.so (__pthread_start(void*)+36)
runtime.cc:523] native: #09 pc 000000000001ec18 /system/lib64/libc.so (__start_thread+68)
runtime.cc:523] (no managed stack frames)
runtime.cc:523]
runtime.cc:523] "Binder:5166_2" prio=10 tid=10 Native
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x138403b8 self=0x77cd82b800
runtime.cc:523] | sysTid=5181 nice=0 cgrp=default sched=0/0 handle=0x77c11ea4f0
runtime.cc:523] | state=S schedstat=( 4266190171 645382344 46830 ) utm=108 stm=317 core=7 HZ=100
runtime.cc:523] | stack=0x77c10f0000-0x77c10f2000 stackSize=1005KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: binder_ioctl_write_read+0x34dc/0x41d4
runtime.cc:523] kernel: binder_ioctl+0x2b4/0xa9c
runtime.cc:523] kernel: do_vfs_ioctl+0x434/0x884
runtime.cc:523] kernel: SyS_ioctl+0x88/0x94
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000006a558 /system/lib64/libc.so (__ioctl+4)
runtime.cc:523] native: #01 pc 0000000000023ebc /system/lib64/libc.so (ioctl+136)
runtime.cc:523] native: #02 pc 000000000054938 /system/lib64/libbinder.so (android::IPCThreadState::talkWithDriver(bool)+260)
runtime.cc:523] native: #03 pc 0000000000054aa8 /system/lib64/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+24)
runtime.cc:523] native: #04 pc 000000000005516c /system/lib64/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+60)
runtime.cc:523] native: #05 pc 000000000007615c /system/lib64/libbinder.so (???)
runtime.cc:523] native: #06 pc 000000000011478 /system/lib64/libutils.so (android::Thread::_threadLoop(void*)+280)
runtime.cc:523] native: #07 pc 00000000000a9814 /system/lib64/libandroid_runtime.so (android::AndroidRuntime::javaThreadShell(void*)+140)
runtime.cc:523] native: #08 pc 0000000000067d80 /system/lib64/libc.so (__pthread_start(void*)+36)
```

```
runtime.cc:523] native: #09 pc 000000000001ec18 /system/lib64/libc.so (__start_thread+68)
runtime.cc:523] (no managed stack frames)
runtime.cc:523]
runtime.cc:523] "Profile Saver" prio=10 tid=11 Native
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x13840440 self=0x77cad08800
runtime.cc:523] | sysTid=5247 nice=9 cgrp=default sched=0/0 handle=0x77c0ecf4f0
runtime.cc:523] | state=S schedstat=( 18938387 450991 10 ) utm=0 stm=0 core=4 HZ=100
runtime.cc:523] | stack=0x77c0dd5000-0x77c0dd7000 stackSize=1005KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: futex_wait_queue_me+0xc4/0x12c
runtime.cc:523] kernel: futex_wait+0xe8/0x2d0
runtime.cc:523] kernel: do_futex+0xf8/0x1408
runtime.cc:523] kernel: SyS_futex+0x144/0x19c
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000001d4ac /system/lib64/libc.so (syscall+28)
runtime.cc:523] native: #01 pc 00000000000e663c /system/lib64/libart.so (art::ConditionVariable::WaitHoldingLocks(art::Thread*)+152)
runtime.cc:523] native: #02 pc 00000000003367c8 /system/lib64/libart.so (art::ProfileSaver::Run()+360)
runtime.cc:523] native: #03 pc 00000000003393b4 /system/lib64/libart.so (art::ProfileSaver::RunProfileSaverThread(void*)+92)
10-08 03:08:32.709 5166-5166/com.xxx.st.vt.test.test A/zygote64: runtime.cc:523] native: #04 pc 0000000000067d80 /system/lib64/libc.so (__pthread_start(void*)+36)
runtime.cc:523] native: #05 pc 000000000001ec18 /system/lib64/libc.so (__start_thread+68)
runtime.cc:523] (no managed stack frames)
runtime.cc:523]
runtime.cc:523] "HwBinder:5166_1" prio=10 tid=13 Native
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x14200098 self=0x77cd832600
runtime.cc:523] | sysTid=5275 nice=-16 cgrp=default sched=0/0 handle=0x77bf3ed4f0
runtime.cc:523] | state=S schedstat=( 10258479647 789208639 59680 ) utm=405 stm=619 core=5 HZ=100
runtime.cc:523] | stack=0x77bf2f3000-0x77bf2f5000 stackSize=1005KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: binder_ioctl_write_read+0x34dc/0x41d4
runtime.cc:523] kernel: binder_ioctl+0x2b4/0xa9c
runtime.cc:523] kernel: do_vfs_ioctl+0x434/0x884
runtime.cc:523] kernel: SyS_ioctl+0x88/0x94
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000006a558 /system/lib64/libc.so (__ioctl+4)
runtime.cc:523] native: #01 pc 0000000000023ebc /system/lib64/libc.so (ioctl+136)
runtime.cc:523] native: #02 pc 000000000014e90 /system/lib64/libhwBinder.so (android::hardware::IPCThreadState::talkWithDriver(bool)+260)
runtime.cc:523] native: #03 pc 0000000000015000 /system/lib64/libhwBinder.so (android::hardware::IPCThreadState::getAndExecuteCommand()+24)
runtime.cc:523] native: #04 pc 0000000000015794 /system/lib64/libhwBinder.so (android::hardware::IPCThreadState::joinThreadPool(bool)+60)
runtime.cc:523] native: #05 pc 000000000001f9b8 /system/lib64/libhwBinder.so (???)
runtime.cc:523] native: #06 pc 0000000000011478 /system/lib64/libutils.so (android::Thread::_threadLoop(void*)+280)
runtime.cc:523] native: #07 pc 00000000000a9814 /system/lib64/libandroid_runtime.so (android::AndroidRuntime::javaThreadShell(void*)+140)
runtime.cc:523] native: #08 pc 0000000000067d80 /system/lib64/libc.so (__pthread_start(void*)+36)
runtime.cc:523] native: #09 pc 000000000001ec18 /system/lib64/libc.so (__start_thread+68)
runtime.cc:523] (no managed stack frames)
runtime.cc:523]
runtime.cc:523] "Binder:5166_3" prio=10 tid=14 Native
runtime.cc:523] | group="" sCount=1 dsCount=0 flags=1 obj=0x14200120 self=0x77cac93e00
runtime.cc:523] | sysTid=11641 nice=0 cgrp=default sched=0/0 handle=0x77befff4f0
runtime.cc:523] | state=S schedstat=( 4367744340 663267804 48343 ) utm=108 stm=327 core=5 HZ=100
runtime.cc:523] | stack=0x77bef05000-0x77bef07000 stackSize=1005KB
runtime.cc:523] | held mutexes=
runtime.cc:523] kernel: __switch_to+0xac/0xb8
runtime.cc:523] kernel: binder_ioctl_write_read+0x34dc/0x41d4
runtime.cc:523] kernel: binder_ioctl+0x2b4/0xa9c
runtime.cc:523] kernel: do_vfs_ioctl+0x434/0x884
runtime.cc:523] kernel: SyS_ioctl+0x88/0x94
runtime.cc:523] kernel: __sys_trace_return+0x0/0x4
runtime.cc:523] native: #00 pc 000000000006a558 /system/lib64/libc.so (__ioctl+4)
runtime.cc:523] native: #01 pc 0000000000023ebc /system/lib64/libc.so (ioctl+136)
runtime.cc:523] native: #02 pc 0000000000054938 /system/lib64/libbinder.so (android::IPCThreadState::talkWithDriver(bool)+260)
runtime.cc:523] native: #03 pc 0000000000054aa8 /system/lib64/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+24)
runtime.cc:523] native: #04 pc 000000000005516c /system/lib64/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+60)
runtime.cc:523] native: #05 pc 000000000007615c /system/lib64/libbinder.so (???)
runtime.cc:523] native: #06 pc 0000000000011478 /system/lib64/libutils.so (android::Thread::_threadLoop(void*)+280)
runtime.cc:523] native: #07 pc 00000000000a9814 /system/lib64/libandroid_runtime.so (android::AndroidRuntime::javaThreadShell(void*)+140)
runtime.cc:523] native: #08 pc 0000000000067d80 /system/lib64/libc.so (__pthread_start(void*)+36)
runtime.cc:523] native: #09 pc 000000000001ec18 /system/lib64/libc.so (__start_thread+68)
runtime.cc:523] (no managed stack frames)
runtime.cc:523]
runtime.cc:523] Aborting thread:
runtime.cc:523] "main" prio=10 tid=1 Runnable
runtime.cc:523] | group="" sCount=0 dsCount=0 flags=0 obj=0x728ec610 self=0x77d5e000
runtime.cc:523] | sysTid=5166 nice=-10 cgrp=default sched=0/0 handle=0x785aaea9a8
runtime.cc:523] | state=R schedstat=( 115866471040 3730737292 565367 ) utm=7014 stm=4571 core=4 HZ=100
runtime.cc:523] | stack=0x77fb5d5000-0x77fb5d7000 stackSize=8MB
runtime.cc:523] | held mutexes= "abort lock" "JNI weak global reference table lock" "mutator lock"(shared held)
runtime.cc:523] native: #00 pc 00000000003ccb5c /system/lib64/libart.so (art::DumpNativeStack(std::__1::basic_ostream<char, std::__1::char_traits<char>>&, int, BacktraceMap*, char const
runtime.cc:523] native: #01 pc 000000000049cdf4 /system/lib64/libart.so (art::Thread::DumpStack(std::__1::basic_ostream<char, std::__1::char_traits<char>>&, bool, BacktraceMap*, bool) cc
runtime.cc:523] native: #02 pc 0000000000484758 /system/lib64/libart.so (art::AbortState::DumpThread(std::__1::basic_ostream<char, std::__1::char_traits<char>>&, art::Thread*) const+56)
runtime.cc:523] native: #03 pc 0000000000484474 /system/lib64/libart.so (art::AbortState::Dump(std::__1::basic_ostream<char, std::__1::char_traits<char>>&) const+500)
runtime.cc:523] native: #04 pc 000000000047598c /system/lib64/libart.so (art::Runtime::Abort(char const*)+196)
runtime.cc:523] native: #05 pc 000000000056b3ec /system/lib64/libart.so (android::base::LogMessage::~~LogMessage()+1004)
runtime.cc:523] native: #06 pc 0000000000263778 /system/lib64/libart.so (art::IndirectReferenceTable::Add(art::IRTSegmentState, art::ObjPtr<art::mirror::Object>)+764)
runtime.cc:523] native: #07 pc 00000000002fecdc /system/lib64/libart.so (art::JavaVMExt::AddWeakGlobalRef(art::Thread*, art::ObjPtr<art::mirror::Object>)+68)
```


runtime.cc:523] native: #08 pc 0000000000385100 /system/lib64/libart.so (art::JNI::NewWeakGlobalRef(_JNIEnv*, _jobject*)+572)
runtime.cc:523] native: #09 pc 000000000010eb80 /system/lib64/libart.so (art::CheckJNI::NewRef(char const*, _JNIEnv*, _jobject*, art::IndirectRefKind)+704)
runtime.cc:523] native: #10 pc 000000000002b220 /system/lib64/libmedia_jni.so (android::JMediaCodec::JMediaCodec(_JNIEnv*, _jobject*, char const*, bool, bool)+248)
runtime.cc:523] native: #11 pc 0000000000030800 /system/lib64/libmedia_jni.so (???)
runtime.cc:523] native: #12 pc 00000000007123c8 /system/framework/arm64/boot-framework.oat (Java_android_media_MediaCodec_native_1setup__Ljava_lang_String_2ZZ+168)
runtime.cc:523] at android.media.MediaCodec.native_setup(Native method)
runtime.cc:523] at android.media.MediaCodec.<init>(MediaCodec.java:1794)
runtime.cc:523] at android.media.MediaCodec.createEncoderByType(MediaCodec.java:1760)
runtime.cc:523] at com.xxx.st.vs.test.test.MainActivity.onCreate(MainActivity.java:23)
runtime.cc:523] at android.app.Activity.performCreate(Activity.java:6999)
runtime.cc:523] at android.app.Activity.performCreate(Activity.java:6990)
runtime.cc:523] at android.app.Instrumentation.callActivityOnCreate(Instrumentation.java:1214)
runtime.cc:523] at android.app.ActivityThread.performLaunchActivity(ActivityThread.java:2731)
runtime.cc:523] at android.app.ActivityThread.handleLaunchActivity(ActivityThread.java:2856)
runtime.cc:523] at android.app.ActivityThread.-wrap11(ActivityThread.java:-1)
runtime.cc:523] at android.app.ActivityThread\$H.handleMessage(ActivityThread.java:1589)
runtime.cc:523] at android.os.Handler.dispatchMessage(Handler.java:106)
runtime.cc:523] at android.os.Looper.loop(Looper.java:164)
runtime.cc:523] at android.app.ActivityThread.main(ActivityThread.java:6494)
runtime.cc:523] at java.lang.reflect.Method.invoke(Native method)
runtime.cc:523] at com.android.internal.os.RuntimeInit\$MethodAndArgsCaller.run(RuntimeInit.java:438)
runtime.cc:523] at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:807)
runtime.cc:523]
runtime.cc:531] JNI ERROR (app bug): weak global reference table overflow (max=51200)
runtime.cc:531] weak global reference table dump:
runtime.cc:531] Last 10 entries (of 51199):
runtime.cc:531] 51198: 0x12ec0028 java.lang.Thread
runtime.cc:531] 51197: 0x12e80028 java.lang.Thread
runtime.cc:531] 51196: 0x12e40028 java.lang.Thread
runtime.cc:531] 51195: 0x12e00028 java.lang.Thread
runtime.cc:531] 51194: 0x12dc0028 java.lang.Thread
runtime.cc:531] 51193: 0x12d80028 java.lang.Thread
runtime.cc:531] 51192: 0x12d40028 java.lang.Thread
runtime.cc:531] 51191: 0x12d00028 java.lang.Thread
runtime.cc:531] 51190: 0x12cc0028 java.lang.Thread
runtime.cc:531] 51189: 0x12c80028 java.lang.Thread
runtime.cc:531] Summary:
runtime.cc:531] 5195 of java.lang.Class (5195 unique instances)
runtime.cc:531] 18 of java.lang.Thread (18 unique instances)
runtime.cc:531] 18 of java.lang.DexCache (18 unique instances)
runtime.cc:531] 3 of dalvik.system.PathClassLoader (2 unique instances)
runtime.cc:531] 3 of java.lang.String (3 unique instances)
runtime.cc:531] 2 of java.lang.ThreadGroup (2 unique instances)
runtime.cc:531] 1 of com.xxx.st.vs.test.test.MainActivity
runtime.cc:531] 1 of android.support.v7.app.AppCompatActivityImpl
runtime.cc:531] 1 of android.arch.lifecycle.LifecycleRegistry
runtime.cc:531] 1 of android.support.v4.app.FragmentActivity\$1
runtime.cc:531] 1 of android.support.v4.app.FragmentController
runtime.cc:531] 1 of android.support.v4.util.SparseArrayCompat
runtime.cc:531] 1 of android.support.v4.util.SimpleArrayMap
runtime.cc:531] 1 of java.lang.BootClassLoader
runtime.cc:531] 1 of java.util.ArrayList
runtime.cc:531] 1 of android.app.ContextImpl
runtime.cc:531] 1 of android.app.ActivityThread
runtime.cc:531] 1 of android.os.Handler
runtime.cc:531] 1 of com.android.internal.policy.PhoneWindow
runtime.cc:531] 1 of android.content.pm.ActivityInfo
runtime.cc:531] 1 of android.content.res.Resources

----- beginning of crash

10-08 03:08:32.710 5166-5166/com.xxx.st.vs.test.test A/libc: Fatal signal 6 (SIGABRT), code -6 in tid 5166 (st.vs.test.test), pid 5166 (st.vs.test.test)

✓ Mentioned issues (1)

-- -- " ...e attached a sample application (see MyTest.zip) that triggers the behaviour (weak global reference overflow). You just have to start that app and wait, the [bug_100](#) % happens on a

COMMENTS

 **ku...@google.com** <ku...@google.com>
Assigned to ku...@google.com.

 **ku...@google.com** <ku...@google.com> [#2](#)

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

Steps to reproduce
What steps do others need to take in order to reproduce the issue themselves?

Please provide sample project or apk to reproduce the issue.

Expected output

Could you please explain the expected behavior.

Current output
Could you please explain the current behavior.

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 r

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 'Tak

su...@gmail.com <su...@gmail.com> [#3](#)

I have attached a sample application (see MyTest.zip) that triggers the behaviour (weak global reference overflow). You just have to start that app and wait, the [bug_100%](#) happens on a Pixel!
MediaCodecTest.zip contains the Android bug report.
If you need more input from my side, please let me know

 **deleted**
0 B 

 **deleted**
0 B 

ku...@google.com <ku...@google.com> [#4](#)

Thank you for reporting this issue. We have shared this with our product and engineering team and will update this issue with more information as it becomes available.

ku...@google.com <ku...@google.com> [#5](#)

Status: Won't Fix (Not Reproducible)

Thank you for reporting this issue. We've investigated, but have been unable to reproduce it with the steps provided. If you are able to reproduce the issue again or have additional information

[Deleted User] <[Deleted User]> [#6](#)

delete