IssueTracker Search IssueTracker Sign in

Android Public Tracker 140956410

ART crash

+1 Hotlists (2) Mark as Duplicate

Comments (7) Dependencies Duplicates (0) Blocking (0) Resources (2)

Infeasible Bug P3 + Add Hotlist [AOSP] assigned

STATUS UPDATE No update yet. Edit

DESCRIPTION lu...@gmail.com created issue #1 Sep 13, 2019 05:23PM

I'm running userdebug android 10 builds on my zenfone 6
I'm hitting the following crash in the ART runtime

```
09-13 09:17:36.311 17962 17962 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
09-13 09:17:36.311 17962 17962 F DEBUG   : Build fingerprint:
'asus/I01WD/I01WD:10/QP1A.190711.020/eng.luca.20190913.001811:userdebug/test-keys'
09-13 09:17:36.311 17962 17962 F DEBUG   : Revision: '0'
09-13 09:17:36.311 17962 17962 F DEBUG   : ABI: 'arm64'
09-13 09:17:36.312 17962 17962 F DEBUG   : Timestamp: 2019-09-13 09:17:36+0200
09-13 09:17:36.312 17962 17962 F DEBUG   : pid: 17742, tid: 17742, name: ogle.android.gm  >>>
com.google.android.gm <<<
09-13 09:17:36.312 17962 17962 F DEBUG   : uid: 10119
09-13 09:17:36.312 17962 17962 F DEBUG   : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x514fd
09-13 09:17:36.312 17962 17962 F DEBUG   :     x0  0000000000000000  x1  00000000a0769168  x2
 0000000000000177  x3  0000000000000000
09-13 09:17:36.312 17962 17962 F DEBUG   :     x4  0000007adcd43340  x5  0000007a87ef150c  x6
 0000007ff6c7d1d0  x7  0000007ff6c7d1b0
09-13 09:17:36.313 17962 17962 F DEBUG   :     x8  0000000000000803  x9  0000000000050cfa  x10
0000000000000070  x11 0000007ac0000000
09-13 09:17:36.313 17962 17962 F DEBUG   :     x12 0000000000000008  x13 000000003f2f3f0  x14
000000000000005b  x15 0000007b7073d09c
09-13 09:17:36.313 17962 17962 F DEBUG   :     x16 0000007b70eda8f0  x17 0000007b70ecc3bc  x18
0000007b7389a000  x19 000000001433e9f0
09-13 09:17:36.313 17962 17962 F DEBUG   :     x20 00000000a0769168  x21 0000007aed5fd000  x22
0000007b72576070  x23 0000007ff6c7d29c
09-13 09:17:36.313 17962 17962 F DEBUG   :     x24 0000007ff6c7d534  x25 0000000000000000  x26
0000007b72576070  x27 0000007aed5fd000
09-13 09:17:36.313 17962 17962 F DEBUG   :     x28 0000000000000004  x29 0000007ff6c7d230
09-13 09:17:36.313 17962 17962 F DEBUG   :     sp  0000007ff6c7d210  lr  0000007aed424540  pc
 0000007aed4245a8
09-13 09:17:36.471 17962 17962 F DEBUG   :
09-13 09:17:36.471 17962 17962 F DEBUG   : backtrace:
09-13 09:17:36.471 17962 17962 F DEBUG   :       #00 pc 00000000003e15a8
 /apex/com.android.runtime/lib64/libart.so
(art::mirror::Class::SetDexCache(art::ObjPtr<art::mirror::DexCache>)+144) (BuildId:
af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.471 17962 17962 F DEBUG   :       #01 pc 000000000016472c
 /apex/com.android.runtime/lib64/libart.so (art::ClassLinker::DefineClass(art::Thread*, char const*, unsigned
long, art::Handle<art::mirror::ClassLoader>, art::DexFile const&, art::dex::ClassDef const&)+488) (BuildId:
af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.471 17962 17962 F DEBUG   :       #02 pc 000000000018dbf8
 /apex/com.android.runtime/lib64/libart.so
(_ZN3art27VisitClassLoaderDexElementsIZNS_24VisitClassLoaderDexFilesIZNS_24VisitClassLoaderDexFilesIZ
NS_11ClassLinker38FindClassInBaseDexClassLoaderClassPathERNS_33ScopedObjectAccessAlreadyRunnable
EPKcmNS_6HandleINS_6mirror11ClassLoaderEEEE4$_31EEvS5_SB_T_EUlPKNS_7DexFileEPPvE_SH_EET0_S5_
SB_SD_SK_EUlNS_6ObjPtrINS9_6ObjectEEESI_E_SH_EESK_S5_SB_SD_SK_+628) (BuildId:
af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.471 17962 17962 F DEBUG   :       #03 pc 0000000000163b74
 /apex/com.android.runtime/lib64/libart.so
(art::ClassLinker::FindClassInBaseDexClassLoader(art::ScopedObjectAccessAlreadyRunnable&, art::Thread*,
char const*, unsigned long, art::Handle<art::mirror::ClassLoader>, art::ObjPtr<art::mirror::Class>*)+684) (BuildId:
af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.471 17962 17962 F DEBUG   :       #04 pc 00000000004243fc
 /apex/com.android.runtime/lib64/libart.so (art::VMClassLoader_findLoadedClass(_JNIEnv*, _jclass*, _jobject*,
_jstring*)+664) (BuildId: af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.471 17962 17962 F DEBUG   :       #05 pc 000000000004c4e8  /system/framework/arm64/boot-
core-libart.oat (art_jni_trampoline+200) (BuildId: 112cc50f5debf03a52d444c07f0425ab1db034a5)
09-13 09:17:36.471 17962 17962 F DEBUG   :       #06 pc 00000000000d1024
 /system/framework/arm64/boot.oat (java.lang.ClassLoader.loadClass+100) (BuildId:
4c00322349a034fde458de3e3f7bbbca4ca7fc68)
```

Reporter	○ lu...@gmail.com
Type	Bug
Priority	P3
Severity	S3
Status	Won't fix (Infeasible)
Access	Default access View
Assignee	○ vi...@google.com
Verifier	--
Collaborators	
CC	lu...@gmail.com
AOSP ID	--
ReportedBy	--
Found In	--
Targeted To	--
Verified In	--
In Prod	○

```
09-13 09:17:36.471 17962 17962 F DEBUG   :       #07 pc 00000000000d0f94
 /system/framework/arm64/boot.oat (java.lang.ClassLoader.loadClass+52) (BuildId:
4c00322349a034fde458de3e3f7bbbca4ca7fc68)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #08 pc 00000000003c5c54  /system/framework/arm64/boot-
framework.oat (android.app.AppComponentFactory.instantiateReceiver+68) (BuildId:
bede8bfb517345cfc21fb1589aa9e75f836b1ab2)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #09 pc 00000000004be7e8  /system/framework/arm64/boot-
framework.oat (android.app.ActivityThread.handleReceiver+840) (BuildId:
bede8bfb517345cfc21fb1589aa9e75f836b1ab2)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #10 pc 00000000004b2e08  /system/framework/arm64/boot-
framework.oat (android.app.ActivityThread$H.handleMessage+6664) (BuildId:
bede8bfb517345cfc21fb1589aa9e75f836b1ab2)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #11 pc 00000000007360c4  /system/framework/arm64/boot-
framework.oat (android.os.Handler.dispatchMessage+180) (BuildId:
bede8bfb517345cfc21fb1589aa9e75f836b1ab2)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #12 pc 000000000073976c  /system/framework/arm64/boot-
framework.oat (android.os.Looper.loop+1756) (BuildId: bede8bfb517345cfc21fb1589aa9e75f836b1ab2)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #13 pc 00000000004c20d0  /system/framework/arm64/boot-
framework.oat (android.app.ActivityThread.main+752) (BuildId:
bede8bfb517345cfc21fb1589aa9e75f836b1ab2)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #14 pc 00000000001365b8
 /apex/com.android.runtime/lib64/libart.so (art_quick_invoke_static_stub+568) (BuildId:
af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #15 pc 0000000000145074
 /apex/com.android.runtime/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int,
art::JValue*, char const*)+276) (BuildId: af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #16 pc 00000000004a0f30
 /apex/com.android.runtime/lib64/libart.so (art::(anonymous
namespace)::InvokeWithArgArray(art::ScopedObjectAccessAlreadyRunnable const&, art::ArtMethod*, art::
(anonymous namespace)::ArgArray*, art::JValue*, char const*)+104) (BuildId:
af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #17 pc 00000000004a2958
 /apex/com.android.runtime/lib64/libart.so (art::InvokeMethod(art::ScopedObjectAccessAlreadyRunnable
const&, _jobject*, _jobject*, _jobject*, unsigned long)+1476) (BuildId: af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #18 pc 0000000000431010
 /apex/com.android.runtime/lib64/libart.so (art::Method_invoke(_JNIEnv*, _jobject*, _jobject*,
_jobjectArray*)+52) (BuildId: af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #19 pc 00000000000bfc34
 /system/framework/arm64/boot.oat (art_jni_trampoline+180) (BuildId:
4c00322349a034fde458de3e3f7bbbca4ca7fc68)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #20 pc 00000000009ab248  /system/framework/arm64/boot-
framework.oat (com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run+136) (BuildId:
bede8bfb517345cfc21fb1589aa9e75f836b1ab2)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #21 pc 00000000009b2ee4  /system/framework/arm64/boot-
framework.oat (com.android.internal.os.ZygoteInit.main+2084) (BuildId:
bede8bfb517345cfc21fb1589aa9e75f836b1ab2)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #22 pc 00000000001365b8
 /apex/com.android.runtime/lib64/libart.so (art_quick_invoke_static_stub+568) (BuildId:
af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #23 pc 0000000000145074
 /apex/com.android.runtime/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int,
art::JValue*, char const*)+276) (BuildId: af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #24 pc 00000000004a0f30
 /apex/com.android.runtime/lib64/libart.so (art::(anonymous
namespace)::InvokeWithArgArray(art::ScopedObjectAccessAlreadyRunnable const&, art::ArtMethod*, art::
(anonymous namespace)::ArgArray*, art::JValue*, char const*)+104) (BuildId:
af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #25 pc 00000000004a0b9c
 /apex/com.android.runtime/lib64/libart.so (art::InvokeWithVarArgs(art::ScopedObjectAccessAlreadyRunnable
const&, _jobject*, _jmethodID*, std::__va_list)+408) (BuildId: af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #26 pc 00000000003b1df0
 /apex/com.android.runtime/lib64/libart.so (art::JNI::CallStaticVoidMethodV(_JNIEnv*, _jclass*, _jmethodID*,
std::__va_list)+764) (BuildId: af2110109ca72ab2252f1818289a0259)
09-13 09:17:36.472 17962 17962 F DEBUG   :       #27 pc 00000000000be560
 /system/lib64/libandroid_runtime.so (_JNIEnv::CallStaticVoidMethod(_jclass*, _jmethodID*, ...)+116) (BuildId:
97bd4110080c8108127686b0a940bcdc)
09-13 09:17:36.473 17962 17962 F DEBUG   :       #28 pc 00000000000c13e8
 /system/lib64/libandroid_runtime.so (android::AndroidRuntime::start(char const*,
android::Vector<android::String8> const&, bool)+780) (BuildId: 97bd4110080c8108127686b0a940bcdc)
09-13 09:17:36.473 17962 17962 F DEBUG   :       #29 pc 00000000000034e0  /system/bin/app_process64
(main+1168) (BuildId: febbb8a0ad8567cc187c7f5b0075dc28)
09-13 09:17:36.473 17962 17962 F DEBUG   :       #30 pc 000000000007d444
 /apex/com.android.runtime/lib64/bionic/libc.so (__libc_init+108) (BuildId:
2190624122e7c2126af94a9462ed8592)
```

COMMENTS

All comments ▼ ↓ Oldest first

vi...@google.com <vi...@google.com> #2 Sep 13, 2019 08:06PM

Assigned to vi...@google.com.

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

Steps to reproduce (if any)
What steps are needed to reproduce this issue

Android bug report capturing (kindly share complete bugreport)
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.

Alternate method
After reproducing the issue, navigate to "developer settings", ensure "USB debugging" is enabled, then enable "Bug report shortcut". Capture bug report by holding the power button and selecting the "Take bug report" option.

Note: Please upload the files to google drive and share the folder to android-bugreport@google.com, then share the link here.

lu...@gmail.com <lu...@gmail.com> #3 Sep 13, 2019 08:10PM

Steps to reproduce (if any)
Simply trying a userdebug GSI on a 9.0 treble enabled device

Android bug report capturing (kindly share complete bugreport)
None, device reboots

lo...@gmail.com <lo...@gmail.com> #4 Sep 14, 2019 10:50AM

```
override fun onPictureInPictureModeChanged(isInPictureInPictureMode: Boolean,
                                           newConfig: Configuration) {
    if (isInPictureInPictureMode) {
        // Hide the full-screen UI (controls, etc.) while in picture-in-picture mode.
    } else {
        // Restore the full-screen UI.
    }
}
```

vi...@google.com <vi...@google.com> #5 Dec 10, 2019 08:05PM

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

vi...@google.com <vi...@google.com> #6 Jan 23, 2020 06:47PM

Status: Won't Fix (Infeasible)

It looks like a stray memory write has corrupted CardTable::biased_begin_ and ART has crashed as a result. We can't say for sure and there isn't enough information in the bug to dig deeper.

lu...@gmail.com <lu...@gmail.com> #7 Jan 23, 2020 06:57PM

Thanks anyways, I now can't repro this crash anymore.