

monkey test:system apps native crash due to weak global reference table overflow (max=51200)

+1 3 Hotlists (2) Mark as Duplicate

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

Infeasible Bug P3 + Add Hotlist [AOSP] NotEnoughInformation NeedsInfo

STATUS UPDATE No update yet. Edit

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

Sep 20, 2016 05:56PM

In Monkey test:many system apps crash because of weak global reference table overflow (max=51200)

trace:

21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] JNI ERROR (app bug): weak global reference table overflow (max=51200)
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] weak global reference table dump:
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] Last 10 entries (of 51200):
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51199: 0x1c767868 android.view.RenderNode
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51198: 0x1c767070 android.view.RenderNode
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51197: 0x1c7672f8 android.view.RenderNode
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51196: 0x1c767310 android.view.RenderNode
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51195: 0x1c767d90 android.view.RenderNode
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51194: 0x1c744640 android.view.RenderNode
11-05 21:52:59.169 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51193: 0x1c744868 android.view.RenderNode
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51192: 0x1c744310 android.view.RenderNode
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51191: 0x1c7446d0 android.view.RenderNode
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 51190: 0x1c7447a8 android.view.RenderNode
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] Summary:
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 3 of byte[] (1440 elements) (3 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 3 of byte[] (5016 elements) (3 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 1 of byte[] (6912 elements)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 5 of byte[] (9216 elements) (5 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 4 of byte[] (10080 elements) (4 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 69 of byte[] (14884 elements) (69 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 1 of byte[] (17280 elements)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 1 of byte[] (19886 elements)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 139 of byte[] (20736 elements) (139 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 3 of byte[] (24156 elements) (3 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 39 of byte[] (26244 elements) (39 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 17 of byte[] (26896 elements) (17 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 2 of byte[] (27572 elements) (2 unique instances)
11-05 21:52:59.170 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 2 of byte[] (27648 elements) (2 unique instances)

Reporter cx...@gmail.com
Type Bug
Priority P3
Severity S3
Status Won't fix (Infeasible)
Access Default access View
Assignee --
Verifier --
Collaborators
CC cx...@gmail.com
AOSP ID 222969
ReportedBy Developer
Found In --
Targeted To --
Verified In --
In Prod

11-05 21:52:59.170 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (28182
11-05 21:52:59.170 1285 1285 F art elements) (4 unique instances)	: art/runtime/indirect_reference_table.cc:116]	4 of byte[] (28670
11-05 21:52:59.170 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (32976
11-05 21:52:59.170 1285 1285 F art elements) (9 unique instances)	: art/runtime/indirect_reference_table.cc:116]	9 of byte[] (33264
11-05 21:52:59.170 1285 1285 F art elements) (2 unique instances)	: art/runtime/indirect_reference_table.cc:116]	2 of byte[] (34848
11-05 21:52:59.170 1285 1285 F art elements) (2 unique instances)	: art/runtime/indirect_reference_table.cc:116]	2 of byte[] (35344
11-05 21:52:59.170 1285 1285 F art elements) (48 unique instances)	: art/runtime/indirect_reference_table.cc:116]	48 of byte[] (36864
11-05 21:52:59.170 1285 1285 F art elements) (6 unique instances)	: art/runtime/indirect_reference_table.cc:116]	6 of byte[] (38016
11-05 21:52:59.170 1285 1285 F art elements) (16 unique instances)	: art/runtime/indirect_reference_table.cc:116]	16 of byte[] (40464
11-05 21:52:59.170 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (41760
11-05 21:52:59.170 1285 1285 F art elements) (4 unique instances)	: art/runtime/indirect_reference_table.cc:116]	4 of byte[] (46512
11-05 21:52:59.170 1285 1285 F art elements) (4 unique instances)	: art/runtime/indirect_reference_table.cc:116]	4 of byte[] (46656
11-05 21:52:59.170 1285 1285 F art elements) (2 unique instances)	: art/runtime/indirect_reference_table.cc:116]	2 of byte[] (47808
11-05 21:52:59.170 1285 1285 F art elements) (2 unique instances)	: art/runtime/indirect_reference_table.cc:116]	2 of byte[] (48114
11-05 21:52:59.170 1285 1285 F art elements) (14 unique instances)	: art/runtime/indirect_reference_table.cc:116]	14 of byte[] (56120
11-05 21:52:59.170 1285 1285 F art elements) (23 unique instances)	: art/runtime/indirect_reference_table.cc:116]	23 of byte[] (59536
11-05 21:52:59.170 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (59584
11-05 21:52:59.170 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (60516
11-05 21:52:59.170 1285 1285 F art elements) (8 unique instances)	: art/runtime/indirect_reference_table.cc:116]	8 of byte[] (66960
11-05 21:52:59.170 1285 1285 F art elements) (3 unique instances)	: art/runtime/indirect_reference_table.cc:116]	3 of byte[] (79488
11-05 21:52:59.170 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (81796
11-05 21:52:59.171 1285 1285 F art elements) (102 unique instances)	: art/runtime/indirect_reference_table.cc:116]	102 of byte[] (82944
11-05 21:52:59.171 1285 1285 F art elements) (3 unique instances)	: art/runtime/indirect_reference_table.cc:116]	3 of byte[] (84100
11-05 21:52:59.171 1285 1285 F art elements) (14 unique instances)	: art/runtime/indirect_reference_table.cc:116]	14 of byte[] (104976
11-05 21:52:59.171 1285 1285 F art elements) (2 unique instances)	: art/runtime/indirect_reference_table.cc:116]	2 of byte[] (106276
11-05 21:52:59.171 1285 1285 F art elements) (4 unique instances)	: art/runtime/indirect_reference_table.cc:116]	4 of byte[] (108000
11-05 21:52:59.171 1285 1285 F art elements) (3 unique instances)	: art/runtime/indirect_reference_table.cc:116]	3 of byte[] (112896
11-05 21:52:59.171 1285 1285 F art elements) (2 unique instances)	: art/runtime/indirect_reference_table.cc:116]	2 of byte[] (135424
11-05 21:52:59.171 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (142884
11-05 21:52:59.171 1285 1285 F art elements) (10 unique instances)	: art/runtime/indirect_reference_table.cc:116]	10 of byte[] (147456
11-05 21:52:59.171 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (153664
11-05 21:52:59.171 1285 1285 F art elements) (6 unique instances)	: art/runtime/indirect_reference_table.cc:116]	6 of byte[] (186624
11-05 21:52:59.171 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (190096
11-05 21:52:59.171 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (236196
11-05 21:52:59.171 1285 1285 F art elements) (3 unique instances)	: art/runtime/indirect_reference_table.cc:116]	3 of byte[] (262144
11-05 21:52:59.171 1285 1285 F art elements) (5 unique instances)	: art/runtime/indirect_reference_table.cc:116]	5 of byte[] (270400
11-05 21:52:59.171 1285 1285 F art elements)	: art/runtime/indirect_reference_table.cc:116]	1 of byte[] (331776
11-05 21:52:59.171 1285 1285 F art java.lang.DexCache (15 unique instances)	: art/runtime/indirect_reference_table.cc:116]	15 of
11-05 21:52:59.171 1285 1285 F art	: art/runtime/indirect_reference_table.cc:116]	3 of

```
dalvik.system.PathClassLoader (2 unique instances)
11-05 21:52:59.171 1285 1285 F art : art/runtime/indirect_reference_table.cc:116] 50581 of
android.view.RenderNode (50581 unique instances)
11-05 21:52:59.171 1285 1285 F art : art/runtime/indirect_reference_table.cc:116]
11-05 21:52:59.171 1285 1285 F art : art/runtime/runtime.cc:405] Runtime aborting...
11-05 21:52:59.171 1285 1285 F art : art/runtime/runtime.cc:405]
----- beginning of crash
11-05 21:52:59.171 1285 1285 F libc : Fatal signal 6 (SIGABRT), code -6 in tid 1285 (ndroid.settings)
11-05 21:52:59.172 338 338 W : debuggerd: handling request: pid=1285 uid=1000 gid=1000 tid=1285
11-05 21:52:59.255 10671 10671 F DEBUG : *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
11-05 21:52:59.255 10671 10671 F DEBUG : Build fingerprint:
'hi3650/hi3650/hi3650:N/NRD81B/3516:eng/test-keys'
11-05 21:52:59.255 10671 10671 F DEBUG : Revision: '0'
11-05 21:52:59.255 10671 10671 F DEBUG : ABL: 'arm64'
11-05 21:52:59.256 10671 10671 F DEBUG : pid: 1285, tid: 1285, name: ndroid.settings >>>
com.android.settings <<<
11-05 21:52:59.256 10671 10671 F DEBUG : signal 6 (SIGABRT), code -6 (SI_TKILL), fault addr -----
11-05 21:52:59.262 10671 10671 F DEBUG : Abort message: 'art/runtime/indirect_reference_table.cc:116] JNI
ERROR (app bug): weak global reference table overflow (max=51200)'
11-05 21:52:59.263 10671 10671 F DEBUG : x0 0000000000000000 x1 0000000000000505 x2
0000000000000006 x3 0000000000000008
11-05 21:52:59.263 10671 10671 F DEBUG : x4 000000000000011a x5 0000800000000000 x6
000000764bbda000 x7 0000000000000000
11-05 21:52:59.263 10671 10671 F DEBUG : x8 0000000000000083 x9 ffffffffdf x10
0000000000000000 x11 0000000000000001
11-05 21:52:59.263 10671 10671 F DEBUG : x12 ffffffff x13 0000000000000000 x14
0000000000000000 x15 00028e98c7f226fc
11-05 21:52:59.263 10671 10671 F DEBUG : x16 0000007648b95ec8 x17 0000007648b3f4ac x18
0000007648b9a010 x19 000000764bc8db40
11-05 21:52:59.263 10671 10671 F DEBUG : x20 0000000000000006 x21 000000764bc8da98 x22
000000000000000b x23 0000000000000d90
11-05 21:52:59.263 10671 10671 F DEBUG : x24 ffffffff x25 0000007647bfc730 x26
0000007647b86a98 x27 0000007feb21d931
11-05 21:52:59.263 10671 10671 F DEBUG : x28 0000007647b4cb8b x29 0000007feb21d860 x30
0000007648b3c954
11-05 21:52:59.263 10671 10671 F DEBUG : sp 0000007feb21d840 pc 0000007648b3f4b4 pstate
0000000060000000
11-05 21:52:59.796 10671 10671 F DEBUG :
11-05 21:52:59.796 10671 10671 F DEBUG : backtrace:
11-05 21:52:59.796 10671 10671 F DEBUG : #00 pc 000000000006b4b4 /system/lib64/libc.so (tgkill+8)
11-05 21:52:59.796 10671 10671 F DEBUG : #01 pc 0000000000068950 /system/lib64/libc.so
(pthread_kill+64)
11-05 21:52:59.796 10671 10671 F DEBUG : #02 pc 0000000000023d28 /system/lib64/libc.so (raise+24)
11-05 21:52:59.796 10671 10671 F DEBUG : #03 pc 000000000001c7ac /system/lib64/libc.so (abort+52)
11-05 21:52:59.797 10671 10671 F DEBUG : #04 pc 0000000000042e9f8 /system/lib64/libart.so
(_ZN3art7Runtime5AbortEv+352)
11-05 21:52:59.797 10671 10671 F DEBUG : #05 pc 00000000000e5358 /system/lib64/libart.so
(_ZN3art10LogMessageD2Ev+1204)
11-05 21:52:59.797 10671 10671 F DEBUG : #06 pc 0000000000253568 /system/lib64/libart.so
(_ZN3art22IndirectReferenceTable3AddEPNS_6mirror6ObjectE+308)
11-05 21:52:59.797 10671 10671 F DEBUG : #07 pc 00000000002ee9a0 /system/lib64/libart.so
(_ZN3art9JavaVMExt16AddWeakGlobalRefEPNS_6ThreadEPNS_6mirror6ObjectE+80)
11-05 21:52:59.797 10671 10671 F DEBUG : #08 pc 0000000000034e23c /system/lib64/libart.so
(_ZN3art3JNI16NewWeakGlobalRefEP7_JNIEnvP8_jobject+600)
11-05 21:52:59.797 10671 10671 F DEBUG : #09 pc 00000000000d8df8
/system/lib64/libandroid_runtime.so
11-05 21:52:59.802 10671 10671 F DEBUG : #10 pc 00000000002266a8c /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.RenderNode.nCreate+152)
11-05 21:52:59.802 10671 10671 F DEBUG : #11 pc 000000000022666d8 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.RenderNode.<init>+84)
11-05 21:52:59.802 10671 10671 F DEBUG : #12 pc 000000000022668a4 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.RenderNode.create+80)
11-05 21:52:59.802 10671 10671 F DEBUG : #13 pc 000000000021c94b4 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.View.<init>+608)
11-05 21:52:59.802 10671 10671 F DEBUG : #14 pc 000000000021c9754 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.View.<init>+112)
11-05 21:52:59.802 10671 10671 F DEBUG : #15 pc 0000000000237bb64 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.widget.TextView.<init>+160)
11-05 21:52:59.802 10671 10671 F DEBUG : #16 pc 0000000000237ba64 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.widget.TextView.<init>+64)
11-05 21:52:59.802 10671 10671 F DEBUG : #17 pc 0000000000237b9d0 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.widget.TextView.<init>+60)
11-05 21:52:59.802 10671 10671 F DEBUG : #18 pc 00000000000d21b4 /system/lib64/libart.so
(art_quick_invoke_stub+580)
11-05 21:52:59.802 10671 10671 F DEBUG : #19 pc 00000000000de80 /system/lib64/libart.so
(_ZN3art9ArtMethod6InvokeEPNS_6ThreadEPjjPNS_6JValueEPKc+204)
11-05 21:52:59.803 10671 10671 F DEBUG : #20 pc 00000000000428340 /system/lib64/libart.so
```

(_ZN3artL18InvokeWithArgArrayERKNS_33ScopedObjectAccessAlreadyRunnableEPNS_9ArtMethodEPNS_8ArgArrayEPNS_6JValueEPKc+108)
11-05 21:52:59.803 10671 10671 F DEBUG : #21 pc 0000000000429eb0 /system/lib64/libart.so
(_ZN3artL12InvokeMethodERKNS_33ScopedObjectAccessAlreadyRunnableEP8_jobjectS4_S4_m+1188)
11-05 21:52:59.803 10671 10671 F DEBUG : #22 pc 0000000000397724 /system/lib64/libart.so
(_ZN3artL24Constructor_newInstance0EP7_JNIEnvP8_jobjectP13_jobjectArray+1244)
11-05 21:52:59.803 10671 10671 F DEBUG : #23 pc 000000000066741c
/system/framework/arm64/boot.oat (offset 0x59e000) (java.lang.reflect.Constructor.newInstance0+152)
11-05 21:52:59.803 10671 10671 F DEBUG : #24 pc 0000000000668330
/system/framework/arm64/boot.oat (offset 0x59e000) (java.lang.reflect.Constructor.newInstance+60)
11-05 21:52:59.803 10671 10671 F DEBUG : #25 pc 0000000002251db0 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.createView+1404)
11-05 21:52:59.803 10671 10671 F DEBUG : #26 pc 00000000025a90d0 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (com.android.internal.policy.PhoneLayoutInflater.onCreateView+140)
11-05 21:52:59.803 10671 10671 F DEBUG : #27 pc 0000000002253b78 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.onCreateView+68)
11-05 21:52:59.803 10671 10671 F DEBUG : #28 pc 0000000002252a30 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.createViewFromTag+972)
11-05 21:52:59.803 10671 10671 F DEBUG : #29 pc 0000000002250758 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.createViewFromTag+68)
11-05 21:52:59.803 10671 10671 F DEBUG : #30 pc 0000000002253f38 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.rInflate+724)
11-05 21:52:59.803 10671 10671 F DEBUG : #31 pc 00000000022542a8 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.rInflateChildren+116)
11-05 21:52:59.803 10671 10671 F DEBUG : #32 pc 0000000002253f9c /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.rInflate+824)
11-05 21:52:59.803 10671 10671 F DEBUG : #33 pc 00000000022542a8 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.rInflateChildren+116)
11-05 21:52:59.803 10671 10671 F DEBUG : #34 pc 00000000022535ec /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.inflate+920)
11-05 21:52:59.804 10671 10671 F DEBUG : #35 pc 0000000002253114 /system/framework/arm64/boot-
framework.oat (offset 0x1668000) (android.view.LayoutInflater.inflate+176)
11-05 21:52:59.804 10671 10671 F DEBUG : #36 pc 00000000006370d0 /data/dalvik-
cache/arm64/system@priv-app@Settings@Settings.apk@classes.dex (offset 0x58c000)

maybe RenderNode cause the bug,please have a look at the bug,thank you!

COMMENTS

All comments

↓ Oldest first



cx...@gmail.com <cx...@gmail.com> [#2](#)

Sep 21, 2016 11:33AM



In RenderNode constructor

```
private RenderNode(String name, View owningView) {  
    mNativeRenderNode = nCreate(name);  
    mOwningView = owningView;  
    if (mOwningView instanceof SurfaceView) {  
        nRequestPositionUpdates(mNativeRenderNode, (SurfaceView) mOwningView);  
    }  
}  
delete -> if (mOwningView instanceof SurfaceView) {  
    nRequestPositionUpdates(mNativeRenderNode, (SurfaceView) mOwningView);  
}  
then monkey test has the problem
```



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

Sep 21, 2016 11:34AM



sorry,the monkey test has no problem



ju...@gmail.com <ju...@gmail.com> [#4](#)

Dec 15, 2016 02:18PM



encounter the same problem. weak global reference table overflow, even the tombstone is the same as yours.
why no update?



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

Dec 15, 2016 11:38PM



Status: New

Hi,
Can you provide the below requested information to better understand the issue:

Android build

Which Android build are you using? (e.g. KVT49L)

Device used

Which device did you use to reproduce this issue?

Device on which monkey test is performed?

Steps to reproduce

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

Please provide monkey test command to test this issue.

Frequency

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

Android bug report:

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.

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



dn...@google.com <dn...@google.com> [#6](#)

Dec 22, 2016 04:16PM ⋮

Please provide the information requested in [comment #5](#) to investigate this issue further.



dn...@google.com <dn...@google.com> [#7](#)

Dec 28, 2016 04:24PM ⋮

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.