signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr deadbaad

+1 21 Hotlists (2) Mark as Duplicate

Comments (14) Dependencies Duplicates (0) Blocking (0) Resources (0)

WAI Bug P3 + Add Hotlist NeedsInfo

STATUS UPDATE No update yet. Edit

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

Feb 3, 2011 03:00PM

Hi, I'm new in Android world and my first project is translate my game engine I wrote in Java to Android (No NDK, all Java :D). All working fine (perhaps framerate is poor at this moment, because I'm using Canvas instead OpenGl), the big problem at this moment are randomly crashes, I think I'm corrupting heap, but don't know where >:(

I'm using emulator with Android 2.1 and 2.3, my phone is Sony Ericcson Xperia X10 mini pro with Android 2.1 too. All devices have same problem.

Steps to reproduce the problem:
- Loading screen (works fine with some IOException, but nothing important to this problem, I solved in my last revision and big problem still here)
- Main menu, you can navigate the menus (Options and Multiplayer)
- New game -> Loading screen again, load resources with no problem
- In game, crash randomly, you can fire, move, or don't do anything, result is the same, i tried going quickly to main menu, sometimes crashes in pause menu, main menu, or navigating to options menu after new game. Problem must be here.

LogCat output:

```
02-03 02:50:14.163 I/DEBUG  (   30): *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***

02-03 02:50:14.163 I/DEBUG  (   30): Build fingerprint: 'generic/sdk/generic:2.3/GRH55/79397:eng/test-keys'

02-03 02:50:14.185 I/DEBUG  (   30): pid: 2760, tid: 2762  >>> javierpastor.gameproject <<<

02-03 02:50:14.185 I/DEBUG  (   30): signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr deadbaad

02-03 02:50:14.203 I/DEBUG  (   30):  r0 deadbaad  r1 0000000c  r2 00000027  r3 00000000

02-03 02:50:14.213 I/DEBUG  (   30):  r4 00000080  r5 afd46668  r6 0000a000  r7 00040006

02-03 02:50:14.213 I/DEBUG  (   30):  r8 100ffab0  r9 415b8f64  10 415b8f50  fp 436169b0

02-03 02:50:14.213 I/DEBUG  (   30):  ip ffffffff  sp 100ffa10  lr afd19375  pc afd15ef0  cpsr 00000030

02-03 02:50:14.703 I/DEBUG  (   30):         #00  pc 00015ef0  /system/lib/libc.so

02-03 02:50:14.713 I/DEBUG  (   30):         #01  pc 00013852  /system/lib/libc.so

02-03 02:50:14.738 I/DEBUG  (   30):

02-03 02:50:14.738 I/DEBUG  (   30): code around pc:

02-03 02:50:14.738 I/DEBUG  (   30): afd15ed0 68241c23 d1fb2c00 68dae027 d0042a00

02-03 02:50:14.743 I/DEBUG  (   30): afd15ee0 20014d18 6028447d 48174790 24802227

02-03 02:50:14.743 I/DEBUG  (   30): afd15ef0 f7f57002 2106eb56 ec92f7f6 0563aa01

02-03 02:50:14.763 I/DEBUG  (   30): afd15f00 60932100 91016051 1c112006 e818f7f6

02-03 02:50:14.783 I/DEBUG  (   30): afd15f10 2200a905 f7f62002 f7f5e824 2106eb42

02-03 02:50:14.783 I/DEBUG  (   30):

02-03 02:50:14.783 I/DEBUG  (   30): code around lr:

02-03 02:50:14.783 I/DEBUG  (   30): afd19354 b0834a0d 589c447b 26009001 686768a5

02-03 02:50:14.793 I/DEBUG  (   30): afd19364 220ce008 2b005eab 1c28d003 47889901
```

Reporter	○ pa...@gmail.com
Type	Bug
Priority	P3
Severity	S3
Status	Won't fix (Intended behavior)
Access	Default access View
Assignee	--
Verifier	--
Collaborators	
CC	pa...@gmail.com
AOSP ID	14498
ReportedBy	Developer
Found In	--
Targeted To	--
Verified In	--
In Prod	○

```
02-03 02:50:14.813 I/DEBUG   (   30): afd19374 35544306 d5f43f01 2c006824 b003d1ee
02-03 02:50:14.813 I/DEBUG   (   30): afd19384 bdf01c30 000281a8 ffffff88 1c0fb5f0
02-03 02:50:14.823 I/DEBUG   (   30): afd19394 43551c3d a904b087 1c16ac01 604d9004
02-03 02:50:14.823 I/DEBUG   (   30):
02-03 02:50:14.823 I/DEBUG   (   30): stack:
02-03 02:50:14.833 I/DEBUG   (   30):     100ff9d0  00000015
02-03 02:50:14.863 I/DEBUG   (   30):     100ff9d4  afd18407  /system/lib/libc.so
02-03 02:50:14.863 I/DEBUG   (   30):     100ff9d8  afd4270c  /system/lib/libc.so
02-03 02:50:14.863 I/DEBUG   (   30):     100ff9dc  afd426b8  /system/lib/libc.so
02-03 02:50:14.883 I/DEBUG   (   30):     100ff9e0  00000000
02-03 02:50:14.883 I/DEBUG   (   30):     100ff9e4  afd19375  /system/lib/libc.so
02-03 02:50:14.883 I/DEBUG   (   30):     100ff9e8  000000da
02-03 02:50:14.893 I/DEBUG   (   30):     100ff9ec  afd183d9  /system/lib/libc.so
02-03 02:50:14.913 I/DEBUG   (   30):     100ff9f0  000001b4
02-03 02:50:14.913 I/DEBUG   (   30):     100ff9f4  00000000
02-03 02:50:14.923 I/DEBUG   (   30):     100ff9f8  afd46668
02-03 02:50:14.923 I/DEBUG   (   30):     100ff9fc  0000a000  [heap]
02-03 02:50:14.923 I/DEBUG   (   30):     100ffa00  00040006  [heap]
02-03 02:50:14.923 I/DEBUG   (   30):     100ffa04  afd18677  /system/lib/libc.so
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa08  df002777
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa0c  e3a070ad
02-03 02:50:14.933 I/DEBUG   (   30): #00 100ffa10  000001b4
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa14  c0000000
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa18  afd46608
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa1c  afd11010  /system/lib/libc.so
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa20  001f5830  [heap]
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa24  fffffbdf
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa28  000000da
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa2c  00000000
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa30  00040008  [heap]
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa34  afd13857  /system/lib/libc.so
02-03 02:50:14.933 I/DEBUG   (   30): #01 100ffa38  00000000
02-03 02:50:14.933 I/DEBUG   (   30):     100ffa3c  afd13857  /system/lib/libc.so
02-03 02:50:14.993 I/DEBUG   (   30):     100ffa40  000000da
02-03 02:50:14.993 I/DEBUG   (   30):     100ffa44  00000110
02-03 02:50:14.993 I/DEBUG   (   30):     100ffa48  000001b4
02-03 02:50:14.993 I/DEBUG   (   30):     100ffa4c  c0000000
02-03 02:50:14.993 I/DEBUG   (   30):     100ffa50  00000001
02-03 02:50:14.993 I/DEBUG   (   30):     100ffa54  001f5830  [heap]
```

```
02-03 02:50:14.993 I/DEBUG   (   30):    100ffa58  0023b358  [heap]

02-03 02:50:14.993 I/DEBUG   (   30):    100ffa5c  00000000

02-03 02:50:14.993 I/DEBUG   (   30):    100ffa60  415b8f6c

02-03 02:50:14.993 I/DEBUG   (   30):    100ffa64  afd14769  /system/lib/libc.so

02-03 02:50:14.993 I/DEBUG   (   30):    100ffa68  001f5830  [heap]

02-03 02:50:14.993 I/DEBUG   (   30):    100ffa6c  81832b84  /system/lib/libskia.so

02-03 02:50:15.023 I/DEBUG   (   30):    100ffa70  001f5830  [heap]

02-03 02:50:15.023 I/DEBUG   (   30):    100ffa74  81852560  /system/lib/libskia.so

02-03 02:50:15.023 I/DEBUG   (   30):    100ffa78  0023b358  [heap]

02-03 02:50:15.023 I/DEBUG   (   30):    100ffa7c  0023b358  [heap]

02-03 02:50:18.803 I/DEBUG   (   30): ptrace attach failed: Operation not permitted

02-03 02:50:18.833 D/Zygote  (   32): Process 2760 terminated by signal (11)

02-03 02:50:18.853 I/ActivityManager(   73): Process javierpastor.gameproject (pid 2760) has died.

02-03 02:50:18.883 E/InputDispatcher(   73): channel '406d3d50
javierpastor.gameproject/javierpastor.gameproject.GameEngine (server)' ~ Consumer closed input channel or
an error occurred.  events=0x8

02-03 02:50:18.883 E/InputDispatcher(   73): channel '406d3d50
javierpastor.gameproject/javierpastor.gameproject.GameEngine (server)' ~ Channel is unrecoverably broken
and will be disposed!

02-03 02:50:18.933 I/WindowManager(   73): WIN DEATH: Window{406d3d50
javierpastor.gameproject/javierpastor.gameproject.GameEngine paused=false}
```

deleted

0 B ⓘ

Restricted

COMMENTS

All comments ▾ | ↓ Oldest first

[Deleted User] <[Deleted User]> #2 Feb 4, 2011 08:47AM ⋮

Address 0xdeadbaad is used by the libc abort() function. It's called by dlmalloc when native heap corruption is detected, but I can't tell if that's what's happening from the backtrace.

Do you have an APK that demonstrates the problem? If you don't have any native code then there is some chance that native crashes are bugs in the platform.

pa...@gmail.com <pa...@gmail.com> #3 Feb 5, 2011 04:01AM ⋮

Yes, I have exported the APK. It´s my test, I must change the images because they can be under copyright, i was using them only for testing, my intention is change them when everything runs OK. APK attached in this comment, thanks for help and sorry for my english.

deleted

0 B ⓘ

Restricted

pa...@gmail.com <pa...@gmail.com> #4 Feb 5, 2011 04:13AM ⋮

I almost forget telling in this test i have performed some changes with UI events in order to avoid flooding but still crashing and framerate has slowdown.
Controls: Movement -> keys W A D Z
        Fire -> Touch the screen in desired direction.

[Deleted User] <[Deleted User]> #5

Feb 10, 2011 05:34AM

I finally got a chance to try it out. I get a lot of input event complaints, and it eventually ANRs, but I haven't seen a native crash.

It seems to take a few seconds to draw a frame.

Note I'm just touching the screen -- my device doesn't have a physical keyboard.

pa...@gmail.com <pa...@gmail.com> #6 Feb 10, 2011 07:04AM

Yes, i read somewhere that touch events should sleep after consuming for avoid flooding, i did it but has result in worse framerate (I will recheck my synchronized functions and list for event handling, event list is filled by UI Thread, but must be readed by game main thread). Try touch screen for fire a few times, and then press back button for get in pause menu, I get a crash when pause menu comes visible, this is the way how I get that stack trace (deadbaad address is the most frecuent crash, I have others, I think the problem must be in same place for these crashes).

Thanks for helping, I will put your name will be in credits [?]. I�m going to make a few tests for get some others crashes examples for post them above here.

[Deleted User] <[Deleted User]> #7 Feb 10, 2011 07:44AM

Looking at "top", you're not burning 100% of the CPU. Watching thread status updates with DDMS shows a "Thread-12" frequently sitting in MONITOR state, i.e. it's waiting on a lock held by another thread. I grabbed a thread dump and it looks like your main thread is in Thread.sleep() (via Engine.onSensorChanged) and the other is in Engine.getPlayerInput; I suspect you've got a stall.

(Note I'm running this on a pre-release device with Honeycomb, so it may be behaving differently from what you're seeing.)

I did what you suggested, firing a couple of times and hitting the back button. After a little over two minutes it did crash:

```
pid: 940, tid: 941  >>> javierpastor.gameproject <<<
signal 7 (SIGBUS), code 128 (?), fault addr 00000000
 r0 ffffffff  r1 001b2cff  r2 00000000  r3 00000001
 r4 ffffffff  r5 001b2cff  r6 00000000  r7 4003af68
 r8 100ffa90  r9 4003af60  10 4003af4c  fp acab1474
 ip ab1f8a24  sp 100ffa48  lr afb049ec  pc afb049ec

Stack Trace:
 RELADDR   FUNCTION                                   FILE:LINE
 000049ec  android_atomic_add+16                          /system/core/include/cutils/atomic-arm.h:158
 v------>  SkBitmap::MipMap::unref()                   /external/skia/src/core/SkBitmap.cpp:75
 00049a14  SkBitmap::freeMipMap()+24                        /external/skia/src/core/SkBitmap.cpp:75
 00049ee8  SkBitmap::freePixels()+8                     /external/skia/src/core/SkBitmap.cpp:338
 00049fa8  SkBitmap::setPixels(void*, SkColorTable*)+16      /external/skia/src/core/SkBitmap.cpp:320
 00054f38  Bitmap_recycle(_JNIEnv*, _jobject*, SkBitmap*)+36
/frameworks/base/core/jni/android/graphics/Bitmap.cpp:268
 00012bfc  dvmPlatformInvoke+124                          /dalvik/vm/arch/arm/CallEABI.S:259
 0004b74e  dvmCallJNIMethod_staticNoRef+62                 /dalvik/vm/Jni.c:1732
 000442a4  dvmCheckCallJNIMethod_staticNoRef+12             /dalvik/vm/CheckJni.c:169
 0001c518  dalvik_mterp+48                              /dalvik/vm/mterp/out/InterpAsm-armv7-a.S:13821

 00020f68  dvmMterpStd+200                               /dalvik/vm/mterp/Mterp.c:109
 0001fef4  dvmInterpret+232                            /dalvik/vm/interp/Interp.c:1361
 000642a8  dvmCallMethodV+296                             /dalvik/vm/interp/Stack.c:531
 000642d0  dvmCallMethod+20                              /dalvik/vm/interp/Stack.c:436
 0005833e  callMethod+86                               /dalvik/vm/alloc/HeapWorker.c:244
 000583b8  doHeapWork+52                                 /dalvik/vm/alloc/HeapWorker.c:307
 00058522  heapWorkerThreadStart+270                          /dalvik/vm/alloc/HeapWorker.c:432
 00056d3e  internalThreadStart+78                         /dalvik/vm/Thread.c:1926
 00011af8  __thread_entry+48                            /bionic/libc/bionic/pthread.c:210
 00011700  pthread_create+184                             /bionic/libc/bionic/pthread.c:350
```

Looks like a failure in Bitmap.recycle().

[Deleted User] <[Deleted User]> #8 Feb 10, 2011 07:53AM

Filed internally as 3439331.

pa...@gmail.com <pa...@gmail.com> #9 Feb 12, 2011 08:49PM

Hello again, I tried delete all recycle() calls in project and "problem has solved", you were right, it must be a bug in recycle, I can now restart game and go to pause menu without problem. I solved another problem, I overrided onBackPressed method for pause menu and go to parent menu instead in onKeyDown method, when Activity called his onPause method, app crashed inmediately after showing menu, if i leave the recycle calls app crash randomly (recycle is called when an actor is deleted because have a temp image where is drawn the sprite in the actual frame). It�s not a pretty good solution but game now works properly, now when finalize method is called i only set null that temp images. Now I have a question �GC will collect that memory like if recycled is called?

If need some more info or the new apk for study the bug, just tell me. Best

di...@gtempaccount.com <di...@gtempaccount.com> #10 Feb 22, 2011 09:15AM

Status: Won't Fix (Intended Behavior)

Not a platform bug. Closing.

[Deleted User] <[Deleted User]> #11 Feb 23, 2011 05:08AM

FWIW, this is still under investigation.

[Deleted User] <[Deleted User]> #12 Feb 24, 2011 11:32AM

The engineer examining the problem concluded:

The APK is using Bitmaps from multiple threads, reusing it after it has been (or while it is being) recycled. The Skia graphics library is not completely thread-safe, and introducing additional synchronization is too expensive, so this won't be fixed in the platform.

So you need to be careful about what you recycle().

un...@gmail.com <un...@gmail.com> #13 Nov 3, 2011 11:07AM

Hi All.

Is there anyone who can share how to get the stack trace like above??

Have a great day.

Thanks.

Stack Trace:

```
  RELADDR   FUNCTION                                    FILE:LINE
  000049ec  android_atomic_add+16                          /system/core/include/cutils/atomic-arm.h:158
  v------>  SkBitmap::MipMap::unref()                   /external/skia/src/core/SkBitmap.cpp:75
  00049a14  SkBitmap::freeMipMap()+24                      /external/skia/src/core/SkBitmap.cpp:75
  00049ee8  SkBitmap::freePixels()+8                    /external/skia/src/core/SkBitmap.cpp:338
  00049fa8  SkBitmap::setPixels(void*, SkColorTable*)+16       /external/skia/src/core/SkBitmap.cpp:320
  00054f38  Bitmap_recycle(_JNIEnv*, _jobject*, SkBitmap*)+36
 /frameworks/base/core/jni/android/graphics/Bitmap.cpp:268
  00012bfc  dvmPlatformInvoke+124                          /dalvik/vm/arch/arm/CallEABI.S:259
```

ca...@gmail.com <ca...@gmail.com> #14 Aug 29, 2014 07:33AM

From your terminal prompt call

```
%> adb logcat -d | ndk-stack -sym $PROJECT_PATH/obj/local/armeabi
```