SIGSEGV opening Animated GIF

Fixed Bug P2 + Add Hotlist OpSys-Android

STATUS UPDATE No update yet. Edit

DESCRIPTION dj...@google.com created issue #1 Jun 6, 2015 05:08AM

Replicating https://crbug.com/skia/173415 from https://code.google.com/p/android/issues/detail?id=173415

SIGSEGV generated while:
Opening a local copy of this animated GIF (I don't own the copyright):
http://www.artisaway.com/wp-content/uploads/2013/02/tijerita.gif

failing on final decodeFile in the following sequence:

```
    options.inJustDecodeBounds = true;
    BitmapFactory.decodeFile(pathName, options);
    options.inJustDecodeBounds = false;
    options.inSampleSize = 3;
unscaledBitmap = BitmapFactory.decodeFile(pathName, options);
```

where options in above line is finally:

```
options = {BitmapFactory$Options@3762}
 inBitmap = null
 inDensity = 0
 inDither = false
 inInputShareable = false
 inJustDecodeBounds = false
 inMutable = false
 inPreferQualityOverSpeed = false
 inPreferredConfig = {Bitmap$Config@3763} "ARGB_8888"
 inPremultiplied = true
 inPurgeable = false
 inSampleSize = 3
 inScaled = true
 inScreenDensity = 0
 inTargetDensity = 0
 inTempStorage = null
 mCancel = false
 outHeight = 500
 outMimeType = {String@3764} "image/gif"
 outWidth = 960
 shadow$_klass_ = {Class@371} "class android.graphics.BitmapFactory$Options"
 shadow$_monitor_ = -1309821806
```

Logcat:

```
05-14 23:35:40.346  25234-25234/com.mamaspells.MamaSpells.full A/libc : Fatal signal 11 (SIGSEGV), code 1, fault addr 0x6b02f000 in tid 25234 (MamaSpells.full)
05-14 23:35:40.447   122-122/? I/DEBUG : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
05-14 23:35:40.447   122-122/? I/DEBUG : Build fingerprint: 'google/nakasi/grouper:5.1.1/LMY47V/1836172:user/release-keys'
05-14 23:35:40.447   122-122/? I/DEBUG : Revision: '0'
05-14 23:35:40.447   122-122/? I/DEBUG : ABI: 'arm'
05-14 23:35:40.448   122-122/? I/DEBUG : pid: 25234, tid: 25234, name: MamaSpells.full >>> com.mamaspells.MamaSpells.full <<<
05-14 23:35:40.448   122-122/? I/DEBUG : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x6b02f000
05-14 23:35:40.461   122-122/? I/DEBUG : r0 6b02ef8c  r1 6a258441  r2 000000fe  r3 00000003
05-14 23:35:40.461   122-122/? I/DEBUG : r4 00000074  r5 6a2585a0  r6 00000140  r7 6b02ef8c
05-14 23:35:40.461   122-122/? I/DEBUG : r8 000001f4  r9 be945638  sl be9455d8  fp 000003c0
05-14 23:35:40.461   122-122/? I/DEBUG : ip 000001f1  sp be945528  lr 40f12429  pc 40f11f96  cpsr 80030030
05-14 23:35:40.462   122-122/? I/DEBUG : backtrace:
05-14 23:35:40.462   122-122/? I/DEBUG : #00 pc 00155f96  /system/lib/libskia.so
05-14 23:35:40.462   122-122/? I/DEBUG : #01 pc 00156427  /system/lib/libskia.so (SkScaledBitmapSampler::sampleInterlaced(unsigned char const*, int)+60)
05-14 23:35:40.462   122-122/? I/DEBUG : #02 pc 00151239  /system/lib/libskia.so (SkGIFImageDecoder::onDecode(SkStream*, SkBitmap*, SkImageDecoder::Mode)+960)
05-14 23:35:40.462   122-122/? I/DEBUG : #03 pc 00150419  /system/lib/libskia.so (SkImageDecoder::decode(SkStream*, SkBitmap*, SkColorType, SkImageDecoder::Mode)+38)
05-14 23:35:40.462   122-122/? I/DEBUG : #04 pc 0008cffb  /system/lib/libandroid_runtime.so
05-14 23:35:40.462   122-122/? I/DEBUG : #05 pc 0008d599  /system/lib/libandroid_runtime.so
05-14 23:35:40.463   122-122/? I/DEBUG : #06 pc 00a41e27  /data/dalvik-cache/arm/system@framework@boot.oat
```

Reporter	dj...@google.com
Type	Bug
Priority	P2
Severity	S2
Status	Fixed
Access	Default access View
Expanded Access	
Assignee	sc...@google.com
Verifier	--
Collaborators	
CC	ms...@google.com
Area	ImageDecoder
Next Action	--
Found In	--
Targeted To	--
Verified In	--
In Prod	

```
05-14 23:35:40.965  475-25349/? W/ActivityManager: Force finishing activity 1
com.mamaspells.MamaSpells.full/com.mamaspells.MamaSpells.WordAdminActivity
05-14 23:35:40.966  122-122/? I/DEBUG: Tombstone written to: /data/tombstones/tombstone_04
05-14 23:35:40.967  475-496/? I/BootReceiver: Copying /data/tombstones/tombstone_04 to DropBox
(SYSTEM_TOMBSTONE)
05-14 23:35:40.993  475-824/? I/WindowState: WIN DEATH: Window{1dc763b1 u0
com.mamaspells.MamaSpells.full/com.mamaspells.MamaSpells.MainActivity}
05-14 23:35:40.996  475-490/? I/WindowState: WIN DEATH: Window{27150e93 u0
com.mamaspells.MamaSpells.full/com.mamaspells.MamaSpells.WordAdminActivity}
05-14 23:35:40.997  475-1223/? I/WindowState: WIN DEATH: Window{258e7d1e u0
com.mamaspells.MamaSpells.full/com.mamaspells.MamaSpells.SettingsActivity}
05-14 23:35:41.030  475-2266/? I/OpenGLRenderer: Initialized EGL, version 1.4
05-14 23:35:41.093  130-130/? I/Zygote: Process 25234 exited due to signal (11)
05-14 23:35:41.133  475-4496/? I/ActivityManager: Process com.mamaspells.MamaSpells.full (pid 25234) has died
05-14 23:35:41.139  475-500/? V/WindowManager: Adding window Window{18ebfefb u0 Starting
com.mamaspells.MamaSpells.full} at 3 of 11 (before Window{27150e93 u0
com.mamaspells.MamaSpells.full/com.mamaspells.MamaSpells.WordAdminActivity EXITING})
05-14 23:35:41.179  475-4496/? I/ActivityManager: Start proc 25353:com.mamaspells.MamaSpells.full/u0a115 for
activity com.mamaspells.MamaSpells.full/com.mamaspells.MamaSpells.SettingsActivity
05-14 23:35:41.180  25353-25353/? I/art: Late-enabling -Xcheck:jni
```

✓ Mentioned issues (1) ✓ Links (4) Hide all

Mentioned issues (1)

--	--	"This sure looks like b/20723696 , which was fixed with https://codereview.chromium.org/1085253002/."	sc...@ #2

Links (4)

"Replicating https://crbug.com/skia/173415 from https://code.google.com/p/android/issues/detail?id=173415"	dj...@ #1
"Replicating https://crbug.com/skia/173415 from https://code.google.com/p/android/issues/detail?id=173415"	dj...@ #1
"http://www.artisaway.com/wp-content/uploads/2013/02... "	dj...@ #1
"This sure looks like b/20723696, which was fixed with https://codereview.chromium.org/1085253002/ ."	sc...@ #2, sc...@ #3

COMMENTS All comments ↓ Oldest first

sc...@google.com <sc...@google.com> #2 Jun 9, 2015 02:01AM

This sure looks like b/20723696, which was fixed with https://codereview.chromium.org/1085253002/.

If so, this is already fixed in MNC. Need to verify though.

sc...@google.com <sc...@google.com> #3 Jun 26, 2015 06:18AM

Marked as fixed.

I have verified that prior to https://codereview.chromium.org/1085253002/, using a sample size of 3 crashes (just running DM), and with that CL, it no longer crashes.