Infeasible Bug P3 + Add Hotlist

STATUS UPDATE No update yet. Edit

DESCRIPTION ma...@gmail.com created issue #1 Oct 10, 2012 11:57PM

Procedure:

1. Launch Stock Browser with url http://tuan.newegg.com.cn in portrait mode.
2. Scroll through the page.
3. Try to switch to landscape mode. scroll through the page.
4. Try to switch to portrait mode. scroll through the page.
5. Repeat 3 & 4 till the browser crashes.

The browser crashes with few trials.

```
I/DEBUG   (  203): *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
I/DEBUG   (  203): Build fingerprint: 'cingular_us/evita/evita:4.0.4/IMM76D/79936.7:user/release-keys'
I/DEBUG   (  203): pid: 8624, tid: 8650  >>> com.android.browser <<<
I/DEBUG   (  203): signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 00000000
I/DEBUG   (  203):  r0 026933f4  r1 02693550  r2 00000001  r3 00000000
I/DEBUG   (  203):  r4 53c288a0  r5 02693470  r6 02693470  r7 53c28820
I/DEBUG   (  203):  r8 027b8230  r9 00000003  10 00000001  fp 53c28890
I/DEBUG   (  203):  ip 00000019  sp 53c28728  lr 509803f7  pc 00000000  cpsr 48000010
I/DEBUG   (  203):  d0  44750000cf000000  d1  4509c00040a00000
I/DEBUG   (  203):  d2  45068000424c0000  d3  4475000044750000
I/DEBUG   (  203):  d4  4506800040a00000  d5  4509c00045068000
I/DEBUG   (  203):  d6  425000004473c000  d7  000000344f000000
I/DEBUG   (  203):  d8  0000000000000000  d9  0000000000000000
I/DEBUG   (  203):  d10 0000000000000000  d11 0000000000000000
I/DEBUG   (  203):  d12 0000000000000000  d13 0000000000000000
I/DEBUG   (  203):  d14 0000000000000000  d15 0000000000000000
I/DEBUG   (  203):  d16 0000000000000000  d17 0000000000000000
I/DEBUG   (  203):  d18 412ad7d000000000  d19 4020000000000000
I/DEBUG   (  203):  d20 3ff0000000000000  d21 8000000000000000
I/DEBUG   (  203):  d22 0000000000000000  d23 bda8fae9be8838d4
I/DEBUG   (  203):  d24 40dd4c2013880000  d25 40ed4c1013880000
I/DEBUG   (  203):  d26 40cd4c4013880000  d27 0000000000000000
I/DEBUG   (  203):  d28 c00005c02b53cb8a  d29 3ff0000000000000
I/DEBUG   (  203):  d30 0000000000000000  d31 3ff0000000000000
I/DEBUG   (  203):  scr 20000013
I/DEBUG   (  203):
I/DEBUG   (  203):         #00  pc 00000000
I/DEBUG   (  203):         #01  pc 001b33f4  /system/lib/libwebcore.so
I/DEBUG   (  203):         #02  pc 001bd332  /system/lib/libwebcore.so
I/DEBUG   (  203):         #03  pc 001bdb32  /system/lib/libwebcore.so
I/DEBUG   (  203):         #04  pc 001bdb62  /system/lib/libwebcore.so
I/DEBUG   (  203):         #05  pc 001bdb62  /system/lib/libwebcore.so
I/DEBUG   (  203):         #06  pc 001bdd74  /system/lib/libwebcore.so
I/DEBUG   (  203):         #07  pc 0023606a  /system/lib/libwebcore.so
I/DEBUG   (  203):         #08  pc 00251b1e  /system/lib/libwebcore.so
I/DEBUG   (  203):         #09  pc 00251b4c  /system/lib/libwebcore.so
I/DEBUG   (  203):         #10  pc 00020070  /system/lib/libdvm.so (dvmPlatformInvoke)
I/DEBUG   (  203):         #11  pc 0005b26c  /system/lib/libdvm.so
(_Z16dvmCallJNIMethodPKjP6JValuePK6MethodP6Thread)
I/DEBUG   (  203):
I/DEBUG   (  203): code around pc:
I/DEBUG   (  203): 00000000 ffffffff ffffffff ffffffff ffffffff  ................
I/DEBUG   (  203): 00000010 ffffffff ffffffff ffffffff ffffffff  ................
I/DEBUG   (  203): 00000020 ffffffff ffffffff ffffffff ffffffff  ................
I/DEBUG   (  203): 00000030 ffffffff ffffffff ffffffff ffffffff  ................
I/DEBUG   (  203): 00000040 ffffffff ffffffff ffffffff ffffffff  ................
I/DEBUG   (  203):
I/DEBUG   (  203): code around lr:
I/DEBUG   (  203): 509803d4 bf00bd70 43f0e92d 20004604 6020460d  p...-..C.F. .F `
I/DEBUG   (  203): 509803e4 6060b08d 60e060a0 680169c8 30b0f8d1  ..``.`.`.i.h...0
```

Reporter ma...@gmail.com
Type Bug
Priority P3
Severity S3
Status Won't fix (Infeasible)
Access Default access View
Assignee --
Verifier --
Collaborators
CC
ma...@gmail.com
AOSP ID 38358
ReportedBy User
Found In --
Targeted To --
Verified In --
In Prod

```
I/DEBUG   (  203): 509803f4 46074798 466eb138 69e94668 fd78f7fd  .G.F8.nFhF.i..x.
I/DEBUG   (  203): 50980404 000fe896 69e8e04a f8d66806 479020e4  ....J..i.h... .G
I/DEBUG   (  203): 50980414 d0322800 46b969e8 fd50f7d5 0810f10d  .(2..i.F..P.....
I/DEBUG   (  203):
I/DEBUG   (  203): stack:
I/DEBUG   (  203):    53c286e8  00000001
I/DEBUG   (  203):    53c286ec  40092473  /system/lib/libc.so
I/DEBUG   (  203):    53c286f0  53c287c0
I/DEBUG   (  203):    53c286f4  508b18bb  /system/lib/libwebcore.so
I/DEBUG   (  203):    53c286f8  53c287c0
I/DEBUG   (  203):    53c286fc  50991ba3  /system/lib/libwebcore.so
I/DEBUG   (  203):    53c28700  53c2872c
I/DEBUG   (  203):    53c28704  00000001
I/DEBUG   (  203):    53c28708  024d05a8  [heap]
I/DEBUG   (  203):    53c2870c  026932d4  [heap]
I/DEBUG   (  203):    53c28710  027b8230  [heap]
I/DEBUG   (  203):    53c28714  509192e5  /system/lib/libwebcore.so
I/DEBUG   (  203):    53c28718  00000000
I/DEBUG   (  203):    53c2871c  50919b7f  /system/lib/libwebcore.so
I/DEBUG   (  203):    53c28720  df0027ad
I/DEBUG   (  203):    53c28724  00000000
/DEBUG   (  203): #01 53c28728  000004f9
I/DEBUG   (  203):    53c2872c  00000000
I/DEBUG   (  203):    53c28730  02692ee4  [heap]
I/DEBUG   (  203):    53c28734  024c4e88  [heap]
I/DEBUG   (  203):    53c28738  02545348  [heap]
I/DEBUG   (  203):    53c2873c  50919b8d  /system/lib/libwebcore.so
I/DEBUG   (  203):    53c28740  02692ee4  [heap]
I/DEBUG   (  203):    53c28744  50989569  /system/lib/libwebcore.so
I/DEBUG   (  203):    53c28748  02692ee4  [heap]
I/DEBUG   (  203):    53c2874c  02545348  [heap]
I/DEBUG   (  203):    53c28750  02692ee4  [heap]
I/DEBUG   (  203):    53c28754  5098a119  /system/lib/libwebcore.so
I/DEBUG   (  203):    53c28758  02692f60  [heap]
I/DEBUG   (  203):    53c2875c  00000004
I/DEBUG   (  203):    53c28760  00000000
I/DEBUG   (  203):    53c28764  02693470  [heap]
I/DEBUG   (  203):    53c28768  53c28820
I/DEBUG   (  203):    53c2876c  027b8230  [heap]
I/DEBUG   (  203):    53c28770  00000003
I/DEBUG   (  203):    53c28774  5098a337  /system/lib/libwebcore.so
```

COMMENTS

All comments ▾ | ↓ Oldest first

[Deleted User] <[Deleted User]> #2 — Oct 11, 2012 12:33PM

This also happens on the Motorola Xoom (wifi only) with Android 4.1.1 (JRO03H). The browser closes without a force close message while scrolling.

ma...@gmail.com <ma...@gmail.com> #3 — Oct 11, 2012 04:31PM

Backtrace:

#1 0x5a0c6254 in WebCore::RenderLayer::localBoundingBox
(ES5_NS_17IdentityExtractorIS5_EENS_28ListHashSetNodeHashFunctionsIS3_Lj256ENS2_8KURLHashE
EENS_10HashTraitsIS5_EESC_EdeEv=Asked for position 0 of stack, stack only has 0 elements on it.
) at external/webkit/./Source/WebCore/rendering/RenderLayer.cpp:3639
#2 0x5a0d516a in WebCore::RenderLayerCompositor::checkForFixedLayers
(ES5_NS_17IdentityExtractorIS5_EENS_28ListHashSetNodeHashFunctionsIS3_Lj256ENS2_8KURLHashE
EENS_10HashTraitsIS5_EESC_EdeEv=Unhandled dwarf expression opcode 0x5
) at external/webkit/./Source/WebCore/rendering/RenderLayerCompositor.cpp:634
#3 0x5a0d57bc in WebCore::RenderLayerCompositor::computeCompositingRequirements
(ES5_NS_17IdentityExtractorIS5_EENS_28ListHashSetNodeHashFunctionsIS3_Lj256ENS2_8KURLHashE
EENS_10HashTraitsIS5_EESC_EdeEv=Unhandled dwarf expression opcode 0x1
) at external/webkit/./Source/WebCore/rendering/RenderLayerCompositor.cpp:801
#4 0x5a0d57f4 in WebCore::RenderLayerCompositor::computeCompositingRequirements
(ES5_NS_17IdentityExtractorIS5_EENS_28ListHashSetNodeHashFunctionsIS3_Lj256ENS2_8KURLHashE
EENS_10HashTraitsIS5_EESC_EdeEv=Unhandled dwarf expression opcode 0x1
) at external/webkit/./Source/WebCore/rendering/RenderLayerCompositor.cpp:806
#5 0x5a0d57f4 in WebCore::RenderLayerCompositor::computeCompositingRequirements
(ES5_NS_17IdentityExtractorIS5_EENS_28ListHashSetNodeHashFunctionsIS3_Lj256ENS2_8KURLHashE
EENS_10HashTraitsIS5_EESC_EdeEv=Unhandled dwarf expression opcode 0x1
) at external/webkit/./Source/WebCore/rendering/RenderLayerCompositor.cpp:806
#6 0x5a0d43d8 in WebCore::RenderLayerCompositor::updateCompositingLayers

(ES5_NS_17IdentityExtractorIS5_EENS_28ListHashSetNodeHashFunctionsIS3_Lj256ENS2_8KURLHashE
EENS_10HashTraitsIS5_EESC_EdeEv=Unhandled dwarf expression opcode 0x1
) at external/webkit/./Source/WebCore/rendering/RenderLayerCompositor.cpp:308
#7 0x5a254a76 in android::ChromeClientAndroid::layersSync
(ES5_NS_17IdentityExtractorIS5_EENS_28ListHashSetNodeHashFunctionsIS3_Lj256ENS2_8KURLHashE
EENS_10HashTraitsIS5_EESC_EdeEv=Remote connection closed
) at external/webkit/./Source/WebKit/android/WebCoreSupport/ChromeClientAndroid.cpp:81
#8 0x5a295628 in android::WebViewCore::updateLayers
(ES5_NS_17IdentityExtractorIS5_EENS_28ListHashSetNodeHashFunctionsIS3_Lj256ENS2_8KURLHashE
EENS_10HashTraitsIS5_EESC_EdeEv=Unhandled dwarf expression opcode 0x0
) at external/webkit/Source/WebKit/android/jni/WebViewCore.cpp:902
#9 0x5a29fc94 in resEE13releaseBufferEv (
=Unhandled dwarf expression opcode 0x0
) at external/webkit/Source/WebKit/android/jni/WebViewCore.cpp:4189
#10 0x40862d34 in dvmPlatformInvoke () at dalvik/vm/arch/arm/CallEABI.S:258
#11 0x4089cc40 in dvmCallJNIMethod (args=Cannot access memory at address 0x5c8b8bf0
) at dalvik/vm/Jni.cpp:1184
#12 0x40890948 in dvmCheckCallJNIMethod (args=<value optimized out>, pResult=0xd87490,
method=0x3d, self=0xd87414) at dalvik/vm/CheckJni.cpp:145
#13 0x40874c10 in dalvik_mterp () at dalvik/vm/mterp/out/InterpAsm-armv7-a-neon.S:26961
#14 0x4087824c in dvmInterpret (self=Cannot access memory at address 0x5c8b8dac
) at dalvik/vm/interp/Interp.cpp:1965
#15 0x408af3d0 in dvmCallMethodV (self=Cannot access memory at address 0x5c8b8e44
) at dalvik/vm/interp/Stack.cpp:522
#16 0x408af3f4 in dvmCallMethod (self=Cannot access memory at address 0x5c8b8e68
) at dalvik/vm/interp/Stack.cpp:425
#17 0x408a2e74 in interpThreadStart (arg=Cannot access memory at address 0x5c8b8e78
) at dalvik/vm/Thread.cpp:1534
#18 0x40084060 in __thread_entry (func=Cannot access memory at address 0x5c8b8ee4
) at bionic/libc/bionic/pthread.c:217
#19 0x40083bb4 in pthread_create (thread_out=<value optimized out>, attr=Cannot access memory at
address 0x5c8b8ef8
) at bionic/libc/bionic/pthread.c:357

#20 0x00448688 in ?? ()
#21 0x00448688 in ?? ()
Backtrace stopped: previous frame identical to this frame (corrupt stack?)

[Deleted User] <[Deleted User]> #4 Oct 19, 2012 12:34AM

The browser still crashes when visiting this site after the update to 4.1.2. Why is Google keeping the stock browser when it is such a buggy piece of junk. They should just get rid of it and replace it with Chrome, although they need to fix it's rendering issues and memory leaks first.

en...@google.com <en...@google.com> Feb 22, 2014 07:31AM

Status: Won't Fix (Infeasible)