App crashed when loading webview url in Activity on Android P device

+1 Hotlists Mark as Duplicate

Comments (6) Dependencies Duplicates (0) Blocking (0) Resources (0)

Infeasible Bug P3 + Add Hotlist

STATUS UPDATE No update yet. Edit

DESCRIPTION ta...@motorolasolutions.com created issue #1 Jun 26, 2019 08:20PM

Device:
Samsung S10 Android P Device >>
Mozilla/5.0 (Linux; Android 9; SM-G973U Build/PPR1.180610.011; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.157 Mobile Safari/537.36

Steps to reproduce:
Start the Activity and load the url in webview.
while loading app got crashed.

Expected behavior
Page should be loaded without crash in system library libminikin.so

What went wrong?
1. EXTJS based Cordova android App.
2. App also contains java code and C library doing lot of app specific operations.
3. Start the New Activity and load the url in webview and while loading app got crashed.
4. backtrace pointing to /system/lib64/libminikin.so

Backtrace:
06-18 20:05:29.820 F/DEBUG (6653): signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x80
06-18 20:05:29.820 F/DEBUG (6653): Cause: null pointer dereference
06-18 20:05:29.820 F/DEBUG (6653): x0 00000071f2d7ae80 x1 0000000000000190 x2 00000071ea2594c0 x3 0000007ffb7efaf8
06-18 20:05:29.820 F/DEBUG (6653): x4 0000000000000000 x5 0000000000000000 x6 0000000000000000 x7 00000071d3d999c1
06-18 20:05:29.820 F/DEBUG (6653): x8 0000000000000080 x9 00000071f2c9f4a0 x10 0000000000000000 x11 0000000000000000
06-18 20:05:29.820 F/DEBUG (6653): x12 0000000042380000 x13 00000000ff000000 x14 0000000000000000 x15 0000000040800000
06-18 20:05:29.820 F/DEBUG (6653): x16 0000007276db7ce0 x17 0000007274f1bf10 x18 0000000000000000 x19 0000007ffb7efa48
06-18 20:05:29.820 F/DEBUG (6653): x20 00000071ea2594c0 x21 0000000013233d80 x22 0000000013233d08 x23 0000000000000000
06-18 20:05:29.820 F/DEBUG (6653): x24 00000072799365f8 x25 0000000000000000 x26 0000000013233d08 x27 0000000013233d80
06-18 20:05:29.820 F/DEBUG (6653): x28 0000000000000000 x29 0000007ffb7efa30
06-18 20:05:29.820 F/DEBUG (6653): sp 0000007ffb7efa00 lr 0000007276cac3b8 pc 0000007274f1bf18
06-18 20:05:29.867 I/sensors-hal(768): handle_sns_std_sensor_event:77, [SSC_LIGHT] physical_light lux: 68, mode: 1, copr: 56, brightness: 107, ts=35087163903626
06-18 20:05:29.867 I/SensorService(1315): [REARLIGHT] lux value : 68, code value : 107
06-18 20:05:29.938 F/DEBUG (6653):
06-18 20:05:29.938 F/DEBUG (6653): backtrace:
06-18 20:05:29.938 F/DEBUG (6653): #00 pc 0000000000017f18 /system/lib64/libminikin.so (minikin::FontCollection::baseFontFaked(minikin::FontStyle)+8)
06-18 20:05:29.938 F/DEBUG (6653): #01 pc 00000000001623b4 /system/lib64/libandroid_runtime.so (android::PaintGlue::getMetricsInternal(long, SkPaint::FontMetrics*)+52)
06-18 20:05:29.938 F/DEBUG (6653): #02 pc 0000000000160edc /system/lib64/libandroid_runtime.so (android::PaintGlue::getFontMetricsInt(_JNIEnv*, _jobject*, long, _jobject*)+56)
06-18 20:05:29.938 F/DEBUG (6653): #03 pc 000000000042b484 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.graphics.Paint.nGetFontMetricsInt [DEDUPED]+180)
06-18 20:05:29.938 F/DEBUG (6653): #04 pc 00000000008866f8 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.graphics.Paint.getFontMetricsInt+56)
06-18 20:05:29.938 F/DEBUG (6653): #05 pc 0000000000ba5b04 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.text.TextLine.expandMetricsFromPaint+84)
06-18 20:05:29.938 F/DEBUG (6653): #06 pc 0000000000ba6068 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.text.TextLine.handleRun+168)
06-18 20:05:29.938 F/DEBUG (6653): #07 pc 0000000000ba7cf8 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.text.TextLine.measure+216)
06-18 20:05:29.938 F/DEBUG (6653): #08 pc 0000000000ba825c /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.text.TextLine.metrics+60)

Reporter ta...@motorolasolutions.com
Type Bug
Priority P3
Severity S3
Status Won't fix (Infeasible)
Access Default access View
Assignee ct...@google.com
Verifier --
Collaborators
CC
ct...@google.com
no...@google.com
ta...@motorolasolutions.com
AOSP ID --
ReportedBy --
Found In --
Targeted To --
Verified In --
In Prod

06-18 20:05:29.938 F/DEBUG (6653): #09 pc 0000000000ca1cc4 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.text.BoringLayout.isBoring+484)
06-18 20:05:29.938 F/DEBUG (6653): #10 pc 0000000000e9402c /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.TextView.makeSingleLayout+284)
06-18 20:05:29.938 F/DEBUG (6653): #11 pc 0000000000e9387c /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.TextView.makeNewLayout+732)
06-18 20:05:29.938 F/DEBUG (6653): #12 pc 0000000000e98798 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.TextView.onMeasure+2600)
06-18 20:05:29.938 F/DEBUG (6653): #13 pc 0000000000cdbfcc /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.View.measure+1276)
06-18 20:05:29.938 F/DEBUG (6653): #14 pc 0000000000da6754 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewGroup.measureChildWithMargins+260)
06-18 20:05:29.938 F/DEBUG (6653): #15 pc 0000000000f0f8c0 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.LinearLayout.measureChildBeforeLayout+64)
06-18 20:05:29.938 F/DEBUG (6653): #16 pc 0000000000f0fe08 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.LinearLayout.measureHorizontal+1288)
06-18 20:05:29.938 F/DEBUG (6653): #17 pc 0000000000f12170 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.LinearLayout.onMeasure+80)
06-18 20:05:29.938 F/DEBUG (6653): #18 pc 0000000000cdbfcc /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.View.measure+1276)
06-18 20:05:29.938 F/DEBUG (6653): #19 pc 0000000000f146d4 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.RelativeLayout.measureChildHorizontal+372)
06-18 20:05:29.938 F/DEBUG (6653): #20 pc 0000000000f15858 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.RelativeLayout.onMeasure+776)
06-18 20:05:29.938 F/DEBUG (6653): #21 pc 0000000000cdbfcc /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.View.measure+1276)
06-18 20:05:29.938 F/DEBUG (6653): #22 pc 0000000000da6754 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewGroup.measureChildWithMargins+260)
06-18 20:05:29.938 F/DEBUG (6653): #23 pc 0000000000f0aa74 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.FrameLayout.onMeasure+340)
06-18 20:05:29.938 F/DEBUG (6653): #24 pc 0000000000cdbfcc /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.View.measure+1276)
06-18 20:05:29.938 F/DEBUG (6653): #25 pc 0000000000da6754 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewGroup.measureChildWithMargins+260)
06-18 20:05:29.938 F/DEBUG (6653): #26 pc 0000000000f0f8c0 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.LinearLayout.measureChildBeforeLayout+64)
06-18 20:05:29.938 F/DEBUG (6653): #27 pc 0000000000f112bc /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.LinearLayout.measureVertical+828)
06-18 20:05:29.938 F/DEBUG (6653): #28 pc 0000000000f12154 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.LinearLayout.onMeasure+52)
06-18 20:05:29.938 F/DEBUG (6653): #29 pc 0000000000cdbfcc /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.View.measure+1276)
06-18 20:05:29.938 F/DEBUG (6653): #30 pc 0000000000da6754 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewGroup.measureChildWithMargins+260)
06-18 20:05:29.938 F/DEBUG (6653): #31 pc 0000000000f0aa74 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.widget.FrameLayout.onMeasure+340)
06-18 20:05:29.938 F/DEBUG (6653): #32 pc 0000000000f4e668 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (com.android.internal.policy.DecorView.onMeasure+1272)
06-18 20:05:29.938 F/DEBUG (6653): #33 pc 0000000000cdbfcc /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.View.measure+1276)
06-18 20:05:29.938 F/DEBUG (6653): #34 pc 0000000000cfda88 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewRootImpl.performMeasure+264)
06-18 20:05:29.938 F/DEBUG (6653): #35 pc 0000000000cfc23c /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewRootImpl.measureHierarchy+1676)
06-18 20:05:29.938 F/DEBUG (6653): #36 pc 0000000000cfe5f4 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewRootImpl.performTraversals+2628)
06-18 20:05:29.938 F/DEBUG (6653): #37 pc 0000000000d04154 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewRootImpl.doTraversal+196)
06-18 20:05:29.938 F/DEBUG (6653): #38 pc 0000000000c0513c /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.ViewRootImpl$TraversalRunnable.run+60)
06-18 20:05:29.938 F/DEBUG (6653): #39 pc 0000000000be8e0c /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.Choreographer.doCallbacks+956)
06-18 20:05:29.938 F/DEBUG (6653): #40 pc 0000000000be971c /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.Choreographer.doFrame+1484)
06-18 20:05:29.938 F/DEBUG (6653): #41 pc 0000000000cb8018 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.view.Choreographer$FrameDisplayEventReceiver.run+72)
06-18 20:05:29.938 F/DEBUG (6653): #42 pc 0000000000b24d2c /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.os.Handler.dispatchMessage+76)
06-18 20:05:29.938 F/DEBUG (6653): #43 pc 0000000000b27e90 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.os.Looper.loop+1264)
06-18 20:05:29.938 F/DEBUG (6653): #44 pc 0000000000901e88 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (android.app.ActivityThread.main+680)
06-18 20:05:29.938 F/DEBUG (6653): #45 pc 000000000055824c /system/lib64/libart.so (art_quick_invoke_static_stub+604)
06-18 20:05:29.938 F/DEBUG (6653): #46 pc 00000000000cfce8 /system/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char const*)+232)
06-18 20:05:29.938 F/DEBUG (6653): #47 pc 000000000045e444 /system/lib64/libart.so (art::(anonymous

namespace)::InvokeWithArgArray(art::ScopedObjectAccessAlreadyRunnable const&, art::ArtMethod*, art::(anonymous namespace)::ArgArray*, art::JValue*, char const*)+104)
06-18 20:05:29.938 F/DEBUG (6653): #48 pc 000000000045fe98 /system/lib64/libart.so (art::InvokeMethod(art::ScopedObjectAccessAlreadyRunnable const&, _jobject*, _jobject*, _jobject*, unsigned long)+1440)
06-18 20:05:29.938 F/DEBUG (6653): #49 pc 00000000003ef51c /system/lib64/libart.so (art::Method_invoke(_JNIEnv*, _jobject*, _jobject*, _jobjectArray*)+52)
06-18 20:05:29.938 F/DEBUG (6653): #50 pc 000000000011f7e4 /system/framework/arm64/boot.oat (offset 0x115000) (java.lang.Class.getDeclaredMethodInternal [DEDUPED]+180)
06-18 20:05:29.938 F/DEBUG (6653): #51 pc 0000000000e0fb48 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run+136)
06-18 20:05:29.938 F/DEBUG (6653): #52 pc 0000000000e166f0 /system/framework/arm64/boot-framework.oat (offset 0x41f000) (com.android.internal.os.ZygoteInit.main+2208)
06-18 20:05:29.938 F/DEBUG (6653): #53 pc 000000000055824c /system/lib64/libart.so (art_quick_invoke_static_stub+604)
06-18 20:05:29.938 F/DEBUG (6653): #54 pc 00000000000cfce8 /system/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char const*)+232)
06-18 20:05:29.938 F/DEBUG (6653): #55 pc 000000000045e444 /system/lib64/libart.so (art::(anonymous namespace)::InvokeWithArgArray(art::ScopedObjectAccessAlreadyRunnable const&, art::ArtMethod*, art::(anonymous namespace)::ArgArray*, art::JValue*, char const*)+104)
06-18 20:05:29.938 F/DEBUG (6653): #56 pc 000000000045e0a4 /system/lib64/libart.so (art::InvokeWithVarArgs(art::ScopedObjectAccessAlreadyRunnable const&, _jobject*, _jmethodID*, std::__va_list)+424)
06-18 20:05:29.938 F/DEBUG (6653): #57 pc 0000000000362d88 /system/lib64/libart.so (art::JNI::CallStaticVoidMethodV(_JNIEnv*, _jclass*, _jmethodID*, std::__va_list)+652)
06-18 20:05:29.938 F/DEBUG (6653): #58 pc 00000000000b9174 /system/lib64/libandroid_runtime.so (_JNIEnv::CallStaticVoidMethod(_jclass*, _jmethodID*, ...)+116)
06-18 20:05:29.938 F/DEBUG (6653): #59 pc 00000000000bbdcc /system/lib64/libandroid_runtime.so (android::AndroidRuntime::start(char const*, android::Vector<android::String8> const&, bool)+768)
06-18 20:05:29.938 F/DEBUG (6653): #60 pc 0000000000004b84 /system/bin/app_process64 (main+1832)
06-18 20:05:29.938 F/DEBUG (6653): #61 pc 00000000000c9e74 /system/lib64/libc.so (__libc_init+88)

COMMENTS

All comments ▾ ↓ Oldest first

ku...@google.com <ku...@google.com> Jul 4, 2019 02:56PM

Assigned to cl...@google.com.

ct...@google.com <ct...@google.com> #2 Aug 1, 2019 08:05AM

Although the bug says it is loading url into WebView, the stack doesn't have any WebView related frame, you'll need to tell us which app are you seeing this stack or maybe providing a sample app to demonstrate the issue. Thanks.

ct...@google.com <ct...@google.com> #3 Aug 1, 2019 08:12AM

This is crashing in minikin, I think TextView team owns it?

ct...@google.com <ct...@google.com> #4 Aug 1, 2019 08:19AM

Reassigned to no...@google.com.

Seigo, could you please take a look, is this a known issue? Please feel free to assign this back to us.

no...@google.com <no...@google.com> #5 Aug 2, 2019 08:51AM

Reassigned to ct...@google.com.

I have no idea.
From the address where crash happens, it looks like there is no families in Typeface, it is unlikely happens with normal API use.

ct...@google.com <ct...@google.com> #6 Aug 2, 2019 10:02AM

Status: Won't Fix (Infeasible)

Thanks Seigo. I don't think this is actionable for WebView team either as the stack isn't in WebView.

tarun.verma@, I am going to close this issue as this is not actionable for us, please provide exact steps to repro this issue with probably sample app in another issue, if you could repro this.