← ↻ ☆   **Code 1 (SEGV_MAPERR) - bug occurring on Android 11 on several devices. After debugging, it does not seem to depend on our code. Please find the build fingerprint below.**   +1 ²⁰ | Hotlists (7) | Mark as Duplicate 🔔 ⋮

Comments (27)   Dependencies   Duplicates (0)   Blocking (0)   Resources (15)

[Fixed] Bug P3 (+)   [AOSP] assigned

👥 **STATUS UPDATE** No update yet.   [Edit]

📄 **DESCRIPTION** en...@gmail.com created issue #1

PLEASE READ:

This form is only for reporting bugs found in the Android system while developing Android applications. Use the Developer Tools subcomponent for issues with the developer tools. https://issuet

Please describe the problem in detail. Be sure to include:

- Steps to reproduce the problem (including sample code if appropriate).
- What happened.
- What you think the correct behavior should be.

Don't forget to mention which version of Android you're using, and/or which device the problem appears on (model and Android version).

Please also run "adb bugreport" and archive the output.

To avoid the possibility of sharing private information, please share bugreports and screenshots from Google Drive. Share files with android-bugreport@google.com and include only Google drive tracker/concepts/restricted-content)" when creating a bug or adding a comment. Restricting or deleting your comment or attachment can also be done using the overflow menu after submitting.

Disclaimer: Please note, by submitting this bug report, you acknowledge that Google may use information included in the bug report to diagnose technical issues and to improve our products and

Bug reports include personal information logged on your device or by apps, such as: File names Installed apps and usage Email addresses of the profiles on the device Device identifiers, such as scanned APNs System or device information, such as memory and processes

---

✓ Mentioned issues (1)   ✓ Links (12)

⚙ **Mentioned issues (1)**

--   --   "https://issuetracker.google.com/201377325"

🔗 **Links (12)**

"This form is only for reporting bugs found in the Android system while developing Android applications. Use the Developer Tools subcomponent for issues with the developer tools. https://issuetrack
"https://developers.google.com/issue-tracker/concepts/res…"
" …te, by submitting this bug report, you acknowledge that Google may use information included in the bug report to diagnose technical issues and to improve our products and services, in accordanc
"For steps to capture a bug report, please refer: https://developer.android.com/studio/debug/bug-report#bugreportdevice"
"https://issuetracker.google.com/components/190923"

    See all related links

COMMENTS

⚪ **en...@gmail.com** <en...@gmail.com> #2

```
# code block
Build fingerprint: 'OPPO/CPH1919EEA/OP4845L1:11/RKQ1.200928.002/1636803154694:user/release-keys'
Revision: '0'
ABI: 'arm64'
Timestamp: 2021-12-23 12:45:06+0100
pid: 13831, tid: 13831, name: es.dev.appname  >>> ferakles.dev.appname <<<
uid: 10320
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x8
Cause: null pointer dereference
    x0  0000000000000000  x1  b400007a9b57836d  x2  fffffffffffffffd  x3  0819081a081b081c
    x4  1c081b081a081908  x5  0819081a081b081c  x6  1c081b081a081908  x7  b400007a88aa3770
    x8  0000007fd1279e20  x9  0000000000000041  x10 b400007a9b578340  x11 b400007a9b578340
    x12 b400007a88aa3b30  x13 b400007a88aa3c70  x14 b400007a88a4ea10  x15 aaaaaaaaaaaaaaab
    x16 0000007b278f45c0  x17 0000007b2b4bc200  x18 0000007b2c632000  x19 0000000000000000
    x20 0000000000000000  x21 b4000079fa60fae0  x22 000000000000003d  x23 000000000000000e
    x24 0000000000000020  x25 b400007a88aa5259  x26 000000000000000e  x27 b400007a88aa5250
    x28 000000000000001b  x29 0000007fd1279f40
    lr  0000007b278c81d4  sp  0000007fd1279dc0  pc  0000007b278c81ec  pst 0000000060000000

backtrace:
      #00 pc 00000000000401ec  /system/lib64/libandroidfw.so (android::Theme::SetTo(android::Theme const&)+2104) (BuildId: dd55aee448a41ca5dd33562f5abdc55
      #01 pc 000000000012209c  /system/lib64/libandroid_runtime.so (android::NativeThemeCopy(_JNIEnv*, _jclass*, long, long, long, long)+132) (BuildId: a5
```

```
#02 pc 000000000021ea50  /system/framework/arm64/boot-framework.oat (art_jni_trampoline+176) (BuildId: 75f57aa82d8d6889edeed86525a613a1631601e4)
#03 pc 00000000001337e8  /apex/com.android.art/lib64/libart.so (art_quick_invoke_static_stub+568) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#04 pc 000000000001a8a94  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char
#05 pc 0000000000318290  /apex/com.android.art/lib64/libart.so (art::interpreter::ArtInterpreterToCompiledCodeBridge(art::Thread*, art::ArtMethod*,
#06 pc 000000000030f67c  /apex/com.android.art/lib64/libart.so (bool art::interpreter::DoCall<true, false>(art::ArtMethod*, art::Thread*, art::Shado
#07 pc 0000000000682a90  /apex/com.android.art/lib64/libart.so (MterpInvokeStaticRange+412) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#08 pc 000000000012dc94  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_static_range+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#09 pc 00000000003b7f00  /system/framework/framework.jar (android.content.res.AssetManager.setThemeTo+28)
#10 pc 00000000006803fc  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtualRange+1132) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#11 pc 000000000012db14  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual_range+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#12 pc 00000000003c3698  /system/framework/framework.jar (android.content.res.ResourcesImpl$ThemeImpl.setTo+28)
#13 pc 00000000067cb78  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+1520) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#14 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#15 pc 00000000003c30c4  /system/framework/framework.jar (android.content.res.Resources$Theme.setTo+8)
#16 pc 00000000067cb78  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+1520) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#17 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#18 pc 00000000001aaa0a  [anon:dalvik-classes.dex extracted in memory from /data/app/~~12f1pinrsH5ib9HaTbdYEQ==/ferakles.dev.appname-PUzrw_OCPgOUhq7
#19 pc 000000000067f1f4  /apex/com.android.art/lib64/libart.so (MterpInvokeDirect+1248) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#20 pc 000000000012d914  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_direct+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#21 pc 00000000001aa87e  [anon:dalvik-classes.dex extracted in memory from /data/app/~~12f1pinrsH5ib9HaTbdYEQ==/ferakles.dev.appname-PUzrw_OCPgOUhq7
#22 pc 00000000067cb78  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+1520) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#23 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#24 pc 000000000027f0a6  /system/framework/framework.jar (offset 0x12ad000) (android.view.ContextThemeWrapper.initializeTheme+46)
#25 pc 000000000067f1f4  /apex/com.android.art/lib64/libart.so (MterpInvokeDirect+1248) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#26 pc 000000000012d914  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_direct+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#27 pc 000000000027f11c  /system/framework/framework.jar (offset 0x12ad000) (android.view.ContextThemeWrapper.setTheme+12)
#28 pc 000000000067d930  /apex/com.android.art/lib64/libart.so (MterpInvokeSuper+2468) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#29 pc 000000000012d894  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_super+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#30 pc 000000000001cf384  /system/framework/framework.jar (android.app.Activity.setTheme)
#31 pc 000000000067d930  /apex/com.android.art/lib64/libart.so (MterpInvokeSuper+2468) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#32 pc 000000000012d894  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_super+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#33 pc 000000000019d0fc  [anon:dalvik-classes.dex extracted in memory from /data/app/~~12f1pinrsH5ib9HaTbdYEQ==/ferakles.dev.appname-PUzrw_OCPgOUhq7
#34 pc 0000000000305bb8  /apex/com.android.art/lib64/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Shado
#35 pc 000000000030dba8  /apex/com.android.art/lib64/libart.so (art::interpreter::ArtInterpreterToInterpreterBridge(art::Thread*, art::CodeItemDataA
#36 pc 000000000030ef90  /apex/com.android.art/lib64/libart.so (bool art::interpreter::DoCall<false, true>(art::ArtMethod*, art::Thread*, art::Shado
#37 pc 0000000000174fb8  /apex/com.android.art/lib64/libart.so (void art::interpreter::ExecuteSwitchImplCpp<true, false>(art::interpreter::SwitchImp
#38 pc 000000000013f7d8  /apex/com.android.art/lib64/libart.so (ExecuteSwitchImplAsm+8) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#39 pc 000000000001bae68  /system/framework/framework.jar (android.app.ActivityThread.performLaunchActivity)
#40 pc 0000000000305cc0  /apex/com.android.art/lib64/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Shado
#41 pc 000000000030dba8  /apex/com.android.art/lib64/libart.so (art::interpreter::ArtInterpreterToInterpreterBridge(art::Thread*, art::CodeItemDataA
#42 pc 000000000030ef90  /apex/com.android.art/lib64/libart.so (bool art::interpreter::DoCall<false, true>(art::ArtMethod*, art::Thread*, art::Shado
#43 pc 0000000000174fb8  /apex/com.android.art/lib64/libart.so (void art::interpreter::ExecuteSwitchImplCpp<true, false>(art::interpreter::SwitchImp
#44 pc 000000000013f7d8  /apex/com.android.art/lib64/libart.so (ExecuteSwitchImplAsm+8) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#45 pc 000000000001bacf8  /system/framework/framework.jar (android.app.ActivityThread.handleLaunchActivity)
#46 pc 0000000000305cc0  /apex/com.android.art/lib64/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Shado
#47 pc 000000000030dba8  /apex/com.android.art/lib64/libart.so (art::interpreter::ArtInterpreterToInterpreterBridge(art::Thread*, art::CodeItemDataA
#48 pc 000000000030e5a0  /apex/com.android.art/lib64/libart.so (bool art::interpreter::DoCall<false, false>(art::ArtMethod*, art::Thread*, art::Shad
#49 pc 000000000067c8d8  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+848) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#50 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#51 pc 000000000002c26ea  /system/framework/framework.jar (android.app.servertransaction.LaunchActivityItem.execute+134)
#52 pc 00000000067cb78  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+1520) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#53 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#54 pc 000000000002c4ada  /system/framework/framework.jar (android.app.servertransaction.TransactionExecutor.executeCallbacks+286)
#55 pc 00000000067cb78  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+1520) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#56 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#57 pc 000000000002c495c  /system/framework/framework.jar (android.app.servertransaction.TransactionExecutor.execute+228)
#58 pc 00000000067cb78  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+1520) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#59 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#60 pc 000000000001b9fe0  /system/framework/framework.jar (android.app.ActivityThread$H.handleMessage+292)
#61 pc 00000000067cb78  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+1520) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#62 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#63 pc 00000000003d141a  /system/framework/framework.jar (offset 0x97a000) (android.os.Handler.dispatchMessage+38)
#64 pc 00000000067cb78  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+1520) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#65 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#66 pc 00000000004039ce  /system/framework/framework.jar (offset 0x97a000) (android.os.Looper.loop+666)
#67 pc 0000000000305bb8  /apex/com.android.art/lib64/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Shado
#68 pc 000000000030dba8  /apex/com.android.art/lib64/libart.so (art::interpreter::ArtInterpreterToInterpreterBridge(art::Thread*, art::CodeItemDataA
#69 pc 000000000030ef90  /apex/com.android.art/lib64/libart.so (bool art::interpreter::DoCall<false, true>(art::ArtMethod*, art::Thread*, art::Shado
#70 pc 0000000000177f40  /apex/com.android.art/lib64/libart.so (void art::interpreter::ExecuteSwitchImplCpp<true, false>(art::interpreter::SwitchImp
#71 pc 000000000013f7d8  /apex/com.android.art/lib64/libart.so (ExecuteSwitchImplAsm+8) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#72 pc 000000000001c57ac  /system/framework/framework.jar (android.app.ActivityThread.main)
#73 pc 0000000000305cc0  /apex/com.android.art/lib64/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Shado
#74 pc 000000000066b5f0  /apex/com.android.art/lib64/libart.so (artQuickToInterpreterBridge+780) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#75 pc 000000000013cff8  /apex/com.android.art/lib64/libart.so (art_quick_to_interpreter_bridge+88) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#76 pc 00000000001337e8  /apex/com.android.art/lib64/libart.so (art_quick_invoke_static_stub+568) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#77 pc 000000000001a8a94  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char
#78 pc 00000000005562bc  /apex/com.android.art/lib64/libart.so (art::InvokeMethod(art::ScopedObjectAccessAlreadyRunnable const&, _jobject*, _jobject
#79 pc 00000000004d53d4  /apex/com.android.art/lib64/libart.so (art::Method_invoke(_JNIEnv*, _jobject*, _jobject*, _jobjectArray*)+52) (BuildId: 0ba
#80 pc 00000000000947f4  /apex/com.android.art/javalib/arm64/boot.oat (art_jni_trampoline+180) (BuildId: f5ff44d4e96af9e82722863cdcbb11a1fae640f2)
#81 pc 0000000000133564  /apex/com.android.art/lib64/libart.so (art_quick_invoke_stub+548) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
```

```
#82 pc 00000000001a8a78  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char
#83 pc 0000000000318290  /apex/com.android.art/lib64/libart.so (art::interpreter::ArtInterpreterToCompiledCodeBridge(art::Thread*, art::ArtMethod*,
#84 pc 000000000030e5bc  /apex/com.android.art/lib64/libart.so (bool art::interpreter::DoCall<false, false>(art::ArtMethod*, art::Thread*, art::Shad
#85 pc 000000000067c8d8  /apex/com.android.art/lib64/libart.so (MterpInvokeVirtual+848) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#86 pc 000000000012d814  /apex/com.android.art/lib64/libart.so (mterp_op_invoke_virtual+20) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#87 pc 00000000005286ba  /system/framework/framework.jar (offset 0x12ad000) (com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run+22)
#88 pc 0000000000305bb8  /apex/com.android.art/lib64/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Shado
#89 pc 000000000066b5f0  /apex/com.android.art/lib64/libart.so (artQuickToInterpreterBridge+780) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#90 pc 000000000013cff8  /apex/com.android.art/lib64/libart.so (art_quick_to_interpreter_bridge+88) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#91 pc 00000000008fac74  /system/framework/arm64/boot-framework.oat (com.android.internal.os.ZygoteInit.main+2756) (BuildId: 75f57aa82d8d6889edeed86
#92 pc 00000000001337e8  /apex/com.android.art/lib64/libart.so (art_quick_invoke_static_stub+568) (BuildId: 0ba3e7738c2ac9a4d1da77e310c0b257)
#93 pc 00000000001a8a94  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char
#94 pc 0000000000554cf8  /apex/com.android.art/lib64/libart.so (art::JValue art::InvokeWithVarArgs<art::ArtMethod*>(art::ScopedObjectAccessAlreadyRu
#95 pc 00000000005551ac  /apex/com.android.art/lib64/libart.so (art::JValue art::InvokeWithVarArgs<_jmethodID*>(art::ScopedObjectAccessAlreadyRunnab
#96 pc 0000000000438fdc  /apex/com.android.art/lib64/libart.so (art::JNI<true>::CallStaticVoidMethodV(_JNIEnv*, _jclass*, _jmethodID*, std::__va_lis
#97 pc 000000000009c424  /system/lib64/libandroid_runtime.so (_JNIEnv::CallStaticVoidMethod(_jclass*, _jmethodID*, ...)+124) (BuildId: a54426a2b2bfe
#98 pc 00000000000a4160  /system/lib64/libandroid_runtime.so (android::AndroidRuntime::start(char const*, android::Vector<android::String8> const&,
#99 pc 0000000000003674  /system/bin/app_process64 (main+1580) (BuildId: 9349370b830e2b77b835dee3aff71480)
#100 pc 0000000000073a5c  /apex/com.android.runtime/lib64/bionic/libc.so (__libc_init+108) (BuildId: 1ca28d785d6567d2b225cf978ef04de5)
```

---

vi...@google.com <vi...@google.com>

Assigned to vi...@google.com.

---

vi...@google.com <vi...@google.com> #3

Thank you for reporting this issue. For us to further investigate this issue, please provide the following additional information:

Apart from OPPO devices, have you observed this issue on Pixel devices ?

Steps to reproduce (include sample apk if needed)
What steps are needed to reproduce this issue?

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

Android bug report (to be captured after reproducing the issue)
For steps to capture a bug report, please refer: https://developer.android.com/studio/debug/bug-report#bugreportdevice

Screen record of the issue
Please capture screen record or video of the issue using following steps:
adb shell screenrecord /sdcard/video.mp4
Subsequently use following command to pull the recorded file:
adb pull /sdcard/video.mp4
Attach the file to this issue.

Capture the issue in a screenshot
Press the volume down and power buttons simultaneously. The image will appear in the picture gallery. Attach the screenshot image to this issue.

Note: Please avoid uploading directly to the issue using attachments. Please upload to google drive and share the folder to android-bugreport@google.com, then share the link here.

---

en...@gmail.com <en...@gmail.com> #4

Hi, thanks for assigning the bug.

- Yes, this issue occurs also on Pixel and Samsung devices.
- Frequency: random, in some cases and with the same device it occurs 10% of the time, in other cases it keeps occurring 100% of times every time we open the app (we also tried restart
- Steps to reproduce: being a random error, it is unfortunately not possible to systematically reproduce it. However, it occurs every time a new fragment or activity is instantiated. By looki

---

vi...@google.com <vi...@google.com> #5

We've shared this with our product and engineering teams and will continue to provide updates as more information becomes available.

---

en...@gmail.com <en...@gmail.com> #6

Ok, thanks. Do not hesitate to let us know if we can provide further info.

---

vi...@google.com <vi...@google.com> #7

Thanks for the above information. For further investigation, we would need few more information about the application and code base information, kindly provide the same.

- **Application**
  - Theme resource name. e.x. R.style.IAmTheme
  - Theme resource id: e.x. 0x7f[0-9a-f]{6}, 0x7f[0-9a-f]{6}, 0x80[0-9a-f]{6}
  - What does the application theme inherit from?
- **Pixel/Emulator**
  - Does the issue happen in a public AOSP emulator?

- if yes, please attachment the bugreport
  - Does the issue happen in Pixel?
    - if yes, please attachment the bugreport

---

en...@gmail.com <en...@gmail.com> #8

Comment has been deleted.

Message last modified on Jan 18, 2022 08:43PM

---

en...@gmail.com <en...@gmail.com> #9

Please find the code regarding the theme:

```
<style name="AppTheme" parent="Theme.MaterialComponents.Light.NoActionBar">
    <item name="colorPrimary">@color/colorPrimary</item>
    <item name="colorPrimaryDark">@color/transparent</item>
    <item name="colorAccent">@color/green</item>
    <item name="android:statusBarColor">@color/transparent</item>
</style>
```

The issue happened in Samsung, Oppo, and also Pixel devices according to Firebase Crashlytics. We use physical devices when developing and it is not possible to replicate the bug systema

---

en...@gmail.com <en...@gmail.com> #10

Hi, do you pls have any news regarding this issue? As additional info, it seems that the bug does not occur on release versions, but only on the debug variants.

---

en...@gmail.com <en...@gmail.com> #11

Hi, do you pls have un update regarding this issue?

---

hy...@gmail.com <hy...@gmail.com> #12

How do i fix this bug

On Mon, Feb 7, 2022, 8:26 AM <buganizer-system@google.com> wrote:

- Show quoted text -

---

vi...@google.com <vi...@google.com> #13

Status: Assigned (reopened)
Comment has been deleted.

---

vi...@google.com <vi...@google.com> #14

Status: Won't Fix (Not Reproducible)

It really sounds like we'll need a bug report from a device this is encountered on to further root cause. Please re-open if you are able to capture a bug report while this happens.

---

en...@gmail.com <en...@gmail.com> #15

Hi, I just generated a bug report from a Samsung device right after the crash occurred, as you requested. But the "re-open" button is disabled on my GUI, despite the fact I am logged with the

---

vi...@google.com <vi...@google.com> #16

Status: Assigned (reopened)

We have re-opened the bug, you may share the bugreport here.

---

vi...@google.com <vi...@google.com> #17

Note: Please avoid uploading directly to the issue using attachments. Please upload to google drive and share the folder to android-bugreport@google.com, then share the link here.

---

en...@gmail.com <en...@gmail.com> #18

Thank you, pls find the link here: https://drive.google.com/drive/folders/1q8ACX0hY849w-ZogKWwbsfxwkuGxckdn?usp=sharing

---

ny...@ukr.net <ny...@ukr.net> #19

Hello. I reduced a new app to a code example that keeps segfaulting:

https://pastebin.com/X5MQxP3L

A NoDisplay activity starts a foreground service and finishes. The service creates an ongoing notification. I tap the notification and it starts another activity. To crash the app somewhat cons

Run it from Android Studio 2021.1.1 Patch 1 on an Android 11 phone. After the notification starts the Crash.java activity, open Crash.java in the studio and press Ctrl+F10 to Apply Changes a few attempts, I get this fault once:

```
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x30000041a00028
    #00 pc 00000000000492b8 /system/lib64/libandroidfw.so (android::LoadedIdmap::IsUpToDate() const+16)
    #01 pc 00000000000306b0 /system/lib64/libandroidfw.so (android::ApkAssets::IsUpToDate() const+32)
    #02 pc 0000000000160dd4 /system/lib64/libandroid_runtime.so (android::NativeIsUpToDate(_JNIEnv*, _jclass*, long)+12)
    #03 pc 00000000001f70e8 /system/framework/arm64/boot-framework.oat
```

After a few more attempts, a different segfault starts appearing:

```
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x8
Cause: null pointer dereference
    #00 pc 000000000003f2a4 /system/lib64/libandroidfw.so (android::Theme::SetTo(android::Theme const&)+2092)
    #01 pc 000000000011edd4 /system/lib64/libandroid_runtime.so (android::NativeThemeCopy(_JNIEnv*, _jclass*, long, long, long, long)+132)
    #02 pc 00000000001f9a50 /system/framework/arm64/boot-framework.oat
```

Restarting the IDE, cleaning and rebuilding the project, rebooting the device and reinstalling the app reduces the error frequency, but doesn't stop it altogether. I confirm these details the topic

Frequency: random, in some cases and with the same device it occurs 10% of the time, in other cases it keeps occurring 100% of times every time we open the app (we also tried restarting

Steps to reproduce: being a random error, it is unfortunately not possible to systematically reproduce it. However, it occurs every time a new fragment or activity is instantiated. By looking

---

kr...@gmail.com <kr...@gmail.com> #20

Hopping on to 'me too' this, I found this thread after encountering the same in my own app too - the trace is similar:
(Samsung galaxy Tab A, Android 11)

```
2022-02-12 20:12:08.790 628-628/? A/DEBUG: Build fingerprint: 'samsung/gta3xlwifieea/gta3xlwifi:11/RP1A.200720.012/T510XXU5CUL1:user/release-keys'
2022-02-12 20:12:08.790 628-628/? A/DEBUG: Revision: '4'
2022-02-12 20:12:08.790 628-628/? A/DEBUG: ABI: 'arm'
2022-02-12 20:12:08.793 628-628/? A/DEBUG: Timestamp: 2022-02-12 20:12:08+0000
2022-02-12 20:12:08.793 628-628/? A/DEBUG: pid: 8510, tid: 8510, name: REDACTED  >>> REDACTED <<<
2022-02-12 20:12:08.793 628-628/? A/DEBUG: uid: 10219
2022-02-12 20:12:08.793 628-628/? A/DEBUG: signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x4
2022-02-12 20:12:08.793 628-628/? A/DEBUG: Cause: null pointer dereference
2022-02-12 20:12:08.793 628-628/? A/DEBUG:   r0 ffa52504 r1 00000000 r2 00000000 r3 00000000
2022-02-12 20:12:08.793 628-628/? A/DEBUG:   r4 00000001 r5 ef068480 r6 ecfe75d5 r7 00000048
2022-02-12 20:12:08.793 628-628/? A/DEBUG:   r8 00000005 r9 ecfe75d0 r10 ecfe75d0 r11 00000008
2022-02-12 20:12:08.793 628-628/? A/DEBUG:   ip ecfe75d5 sp ffa524c0 lr eee6f307 pc eee6f31e
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #00 pc 0002f31e /system/lib/libandroidfw.so (android::Theme::SetTo(android::Theme const&)+1534) (BuildId: 7488d1447c7a8a102067
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #01 pc 000c7707 /system/lib/libandroid_runtime.so (android::NativeThemeCopy(_JNIEnv*, _jclass*, long long, long long, long long, long
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #02 pc 0022d2d1 /system/framework/arm/boot-framework.oat (art_jni_trampoline+152) (BuildId: 6960bf7bbad85d9c21f6fdefcd60f5cf
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #03 pc 000d47d5 /apex/com.android.art/lib/libart.so (art_quick_invoke_stub_internal+68) (BuildId: f7f7992afe026d297489f7304e96a4f
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #04 pc 004f2559 /apex/com.android.art/lib/libart.so (art_quick_invoke_static_stub+276) (BuildId: f7f7992afe026d297489f7304e96a4f2
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #05 pc 0012cb3f /apex/com.android.art/lib/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #06 pc 00245c97 /apex/com.android.art/lib/libart.so (art::interpreter::ArtInterpreterToCompiledCodeBridge(art::Thread*, art::ArtMethod
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #07 pc 0023e611 /apex/com.android.art/lib/libart.so (bool art::interpreter::DoCall<true, false>(art::ArtMethod*, art::Thread*, art::Shadow
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #08 pc 004e910f /apex/com.android.art/lib/libart.so (MterpInvokeStaticRange+370) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.262 628-628/? A/DEBUG:   #09 pc 000cf694 /apex/com.android.art/lib/libart.so (mterp_op_invoke_static_range+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #10 pc 003f53ec /system/framework/framework.jar (android.content.res.AssetManager.setThemeTo+28)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #11 pc 004e6e51 /apex/com.android.art/lib/libart.so (MterpInvokeVirtualRange+996) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #12 pc 000cf514 /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual_range+20) (BuildId: f7f7992afe026d297489f7304e96a4f
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #13 pc 003fcba8 /system/framework/framework.jar (android.content.res.ResourcesImpl$ThemeImpl.setTo+28)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #14 pc 004e3c31 /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+1300) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #15 pc 000cf214 /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #16 pc 003fc1b8 /system/framework/framework.jar (android.content.res.Resources$Theme.setTo+8)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #17 pc 004e3c31 /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+1300) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #18 pc 000cf214 /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #19 pc 0017e116 [anon:dalvik-classes.dex extracted in memory from /data/app/~~4QpeN1F8ZbKlZD2JAvWPjA==/com.precisioncolour
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #20 pc 004e5e01 /apex/com.android.art/lib/libart.so (MterpInvokeDirect+1116) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #21 pc 000cf314 /apex/com.android.art/lib/libart.so (mterp_op_invoke_direct+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #22 pc 0017df8a [anon:dalvik-classes.dex extracted in memory from /data/app/~~4QpeN1F8ZbKlZD2JAvWPjA==/com.precisioncolour
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #23 pc 004e3c31 /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+1300) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.263 628-628/? A/DEBUG:   #24 pc 000cf214 /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #25 pc 002dd326 /system/framework/framework.jar (offset 0x130e000) (android.view.ContextThemeWrapper.initializeTheme+46)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #26 pc 004e5e01 /apex/com.android.art/lib/libart.so (MterpInvokeDirect+1116) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #27 pc 000cf314 /apex/com.android.art/lib/libart.so (mterp_op_invoke_direct+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #28 pc 002dd39c /system/framework/framework.jar (offset 0x130e000) (android.view.ContextThemeWrapper.setTheme+12)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #29 pc 004e4825 /apex/com.android.art/lib/libart.so (MterpInvokeSuper+2032) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #30 pc 000cf294 /apex/com.android.art/lib/libart.so (mterp_op_invoke_super+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #31 pc 001d56ac /system/framework/framework.jar (android.app.Activity.setTheme)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #32 pc 004e4825 /apex/com.android.art/lib/libart.so (MterpInvokeSuper+2032) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #33 pc 000cf294 /apex/com.android.art/lib/libart.so (mterp_op_invoke_super+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #34 pc 001707b0 [anon:dalvik-classes.dex extracted in memory from /data/app/~~4QpeN1F8ZbKlZD2JAvWPjA==/com.precisioncolour
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #35 pc 00236951 /apex/com.android.art/lib/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Sha
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #36 pc 0023d18d /apex/com.android.art/lib/libart.so (art::interpreter::ArtInterpreterToInterpreterBridge(art::Thread*, art::CodeItemData
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #37 pc 0023e0c7 /apex/com.android.art/lib/libart.so (bool art::interpreter::DoCall<false, true>(art::ArtMethod*, art::Thread*, art::Shadow
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #38 pc 001047db /apex/com.android.art/lib/libart.so (void art::interpreter::ExecuteSwitchImplCpp<true, false>(art::interpreter::SwitchIm
```

```
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #39 pc 000d9e75  /apex/com.android.art/lib/libart.so (ExecuteSwitchImplAsm+4) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #40 pc 001c0adc  /system/framework/framework.jar (android.app.ActivityThread.performLaunchActivity)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #41 pc 0023690d  /apex/com.android.art/lib/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Sha
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #42 pc 0023d18d  /apex/com.android.art/lib/libart.so (art::interpreter::ArtInterpreterToInterpreterBridge(art::Thread*, art::CodeItemData,
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #43 pc 0023e0c7  /apex/com.android.art/lib/libart.so (bool art::interpreter::DoCall<false, true>(art::ArtMethod*, art::Thread*, art::Shadow
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #44 pc 001071e5  /apex/com.android.art/lib/libart.so (void art::interpreter::ExecuteSwitchImplCpp<true, false>(art::interpreter::SwitchIm
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #45 pc 000d9e75  /apex/com.android.art/lib/libart.so (ExecuteSwitchImplAsm+4) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #46 pc 001c09c8  /system/framework/framework.jar (android.app.ActivityThread.handleLaunchActivity)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #47 pc 0023690d  /apex/com.android.art/lib/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Sha
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #48 pc 0023d18d  /apex/com.android.art/lib/libart.so (art::interpreter::ArtInterpreterToInterpreterBridge(art::Thread*, art::CodeItemData,
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #49 pc 0023d941  /apex/com.android.art/lib/libart.so (bool art::interpreter::DoCall<false, false>(art::ArtMethod*, art::Thread*, art::Shado
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #50 pc 004e39f5  /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+728) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #51 pc 000cf214  /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #52 pc 002e7036  /system/framework/framework.jar (android.app.servertransaction.LaunchActivityItem.execute+134)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #53 pc 004e3c31  /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+1300) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #54 pc 000cf214  /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #55 pc 002e947a  /system/framework/framework.jar (android.app.servertransaction.TransactionExecutor.executeCallbacks+154)
2022-02-12 20:12:09.264 628-628/? A/DEBUG:   #56 pc 004e3c31  /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+1300) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #57 pc 000cf214  /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #58 pc 002e93b6  /system/framework/framework.jar (android.app.servertransaction.TransactionExecutor.execute+146)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #59 pc 004e3c31  /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+1300) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #60 pc 000cf214  /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #61 pc 001bfd94  /system/framework/framework.jar (android.app.ActivityThread$H.handleMessage+276)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #62 pc 004e3c31  /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+1300) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #63 pc 000cf214  /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #64 pc 0040d3b6  /system/framework/framework.jar (offset 0x9c8000) (android.os.Handler.dispatchMessage+38)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #65 pc 004e3c31  /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+1300) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #66 pc 000cf214  /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #67 pc 0044cef8  /system/framework/framework.jar (offset 0x9c8000) (android.os.Looper.loop+480)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #68 pc 00236951  /apex/com.android.art/lib/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Sha
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #69 pc 0023d18d  /apex/com.android.art/lib/libart.so (art::interpreter::ArtInterpreterToInterpreterBridge(art::Thread*, art::CodeItemData,
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #70 pc 0023e0c7  /apex/com.android.art/lib/libart.so (bool art::interpreter::DoCall<false, true>(art::ArtMethod*, art::Thread*, art::Shadow
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #71 pc 001071e5  /apex/com.android.art/lib/libart.so (void art::interpreter::ExecuteSwitchImplCpp<true, false>(art::interpreter::SwitchIm
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #72 pc 000d9e75  /apex/com.android.art/lib/libart.so (ExecuteSwitchImplAsm+4) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #73 pc 001cb514  /system/framework/framework.jar (android.app.ActivityThread.main)
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #74 pc 0023690d  /apex/com.android.art/lib/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Sha
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #75 pc 0023d0c1  /apex/com.android.art/lib/libart.so (art::interpreter::EnterInterpreterFromEntryPoint(art::Thread*, art::CodeItemDataAc
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #76 pc 004d5233  /apex/com.android.art/lib/libart.so (artQuickToInterpreterBridge+698) (BuildId: f7f7992afe026d297489f7304e96a4f2
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #77 pc 000d9361  /apex/com.android.art/lib/libart.so (art_quick_to_interpreter_bridge+32) (BuildId: f7f7992afe026d297489f7304e96a4
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #78 pc 000d47d5  /apex/com.android.art/lib/libart.so (art_quick_invoke_stub_internal+68) (BuildId: f7f7992afe026d297489f7304e96a4f
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #79 pc 004f2559  /apex/com.android.art/lib/libart.so (art_quick_invoke_static_stub+276) (BuildId: f7f7992afe026d297489f7304e96a4f2
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #80 pc 0012cb3f  /apex/com.android.art/lib/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #81 pc 003ffc1b  /apex/com.android.art/lib/libart.so (art::InvokeMethod(art::ScopedObjectAccessAlreadyRunnable const&, _jobject*, _jo
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #82 pc 003a0173  /apex/com.android.art/lib/libart.so (art::Method_invoke(_JNIEnv*, _jobject*, _jobject*, _jobjectArray*)+30) (BuildId: f7f
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #83 pc 00083667  /apex/com.android.art/javalib/arm/boot.oat (art_jni_trampoline+110) (BuildId: 6843b0dbb04cdc405bffab59f06ecaf31
2022-02-12 20:12:09.265 628-628/? A/DEBUG:   #84 pc 000d47d5  /apex/com.android.art/lib/libart.so (art_quick_invoke_stub_internal+68) (BuildId: f7f7992afe026d297489f7304e96a4f
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #85 pc 004f2427  /apex/com.android.art/lib/libart.so (art_quick_invoke_stub+282) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #86 pc 0012cb2d  /apex/com.android.art/lib/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #87 pc 00245c97  /apex/com.android.art/lib/libart.so (art::interpreter::ArtInterpreterToCompiledCodeBridge(art::Thread*, art::ArtMethod
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #88 pc 0023d957  /apex/com.android.art/lib/libart.so (bool art::interpreter::DoCall<false, false>(art::ArtMethod*, art::Thread*, art::Shado
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #89 pc 004e39f5  /apex/com.android.art/lib/libart.so (MterpInvokeVirtual+728) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #90 pc 000cf214  /apex/com.android.art/lib/libart.so (mterp_op_invoke_virtual+20) (BuildId: f7f7992afe026d297489f7304e96a4f2)
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #91 pc 002334d2  /system/framework/framework.jar (offset 0x1bf0000) (com.android.internal.os.RuntimeInit$MethodAndArgsCaller.ru
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #92 pc 00236951  /apex/com.android.art/lib/libart.so (art::interpreter::Execute(art::Thread*, art::CodeItemDataAccessor const&, art::Sha
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #93 pc 0023d0c1  /apex/com.android.art/lib/libart.so (art::interpreter::EnterInterpreterFromEntryPoint(art::Thread*, art::CodeItemDataAc
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #94 pc 004d5233  /apex/com.android.art/lib/libart.so (artQuickToInterpreterBridge+698) (BuildId: f7f7992afe026d297489f7304e96a4f2
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #95 pc 000d9361  /apex/com.android.art/lib/libart.so (art_quick_to_interpreter_bridge+32) (BuildId: f7f7992afe026d297489f7304e96a4
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #96 pc 0090f137  /system/framework/arm/boot-framework.oat (com.android.internal.os.ZygoteInit.main+2086) (BuildId: 6960bf7bbad8
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #97 pc 000d47d5  /apex/com.android.art/lib/libart.so (art_quick_invoke_stub_internal+68) (BuildId: f7f7992afe026d297489f7304e96a4f
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #98 pc 004f2559  /apex/com.android.art/lib/libart.so (art_quick_invoke_static_stub+276) (BuildId: f7f7992afe026d297489f7304e96a4f2
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #99 pc 0012cb3f  /apex/com.android.art/lib/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #100 pc 003fed77  /apex/com.android.art/lib/libart.so (art::JValue art::InvokeWithVarArgs<art::ArtMethod*>(art::ScopedObjectAccessAl
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #101 pc 003ff01b  /apex/com.android.art/lib/libart.so (art::JValue art::InvokeWithVarArgs<_jmethodID*>(art::ScopedObjectAccessAlread
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #102 pc 00328aad  /apex/com.android.art/lib/libart.so (art::JNI<true>::CallStaticVoidMethodV(_JNIEnv*, _jclass*, _jmethodID*, std::__va
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #103 pc 000694d5  /system/lib/libandroid_runtime.so (_JNIEnv::CallStaticVoidMethod(_jclass*, _jmethodID*, ...)+28) (BuildId: 9b0e90ce
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #104 pc 0006f9a9  /system/lib/libandroid_runtime.so (android::AndroidRuntime::start(char const*, android::Vector<android::String8> co
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #105 pc 00002e55  /system/bin/app_process32 (main+976) (BuildId: 93fc888834cfed5e2c418eec9e7cd580)
2022-02-12 20:12:09.266 628-628/? A/DEBUG:   #106 pc 0005d5b1  /apex/com.android.runtime/lib/bionic/libc.so (__libc_init+68) (BuildId: fef5b751123147ea65bf3f4f798c9518)
```

I've tried invalidating caches, rebuilding and everything the previous poster has also tried.

---

kr...@gmail.com <kr...@gmail.com> #21

Forgot to include theme information:

```
<style name="AppTheme" parent="Theme.AppCompat.Light.NoActionBar">

    <item name="colorAccent">@color/colorAccent</item>

    <item name="windowActionBar">false</item>
    <item name="windowActionBarOverlay">true</item>
    <item name="windowNoTitle">true</item>

    <item name="android:windowContentTransitions">true</item>
    <item name="android:windowActivityTransitions">true</item>
    <item name="android:colorBackground">@color/appBackground</item>
```

```
        <item name="colorPrimary">@color/background1</item>
        <item name="actionBarTheme">@style/AppTheme.AppBarOverlay</item>
        <item name="actionBarPopupTheme">@style/AppTheme.PopupOverlay</item>

    </style>
```

en...@gmail.com <en...@gmail.com> #22

Hi, answering to #19: Thank you for taking the time to investigate the issue. In summary, you found two SEGV_MAPERR crashes. The second SEGV_MAPERR is the one that regards current is

ny...@ukr.net <ny...@ukr.net> #23

#22: Yes and no. The bug is reliably replicable in the public AOSP 11 emulator, whether x86 or ARM. I described the steps to have it occur, but I indeed don't know how to fix it, as I'm an applic

en...@gmail.com <en...@gmail.com> #24

Hi, the status changed back to assigned and I have been asked to upload the bugreport (pls see #18) 4 weeks ago. Can you pls tell me if you were able to investigate it? Thank you

vi...@google.com <vi...@google.com> #25

Comment has been deleted.

vi...@google.com <vi...@google.com> #26

Marked as fixed.

According to the theme defined by the application, there are two suspicious places.

```
        <item name="actionBarTheme">@style/AppTheme.AppBarOverlay</item>
        <item name="actionBarPopupTheme">@style/AppTheme.PopupOverlay</item>
```

The widgets will fetch data from **AppTheme.AppBarOverlay** and **AppTheme.PopupOverlay**. However, Neither **AppTheme.AppBarOverlay** nor **AppTheme.PopupOverlay** inherit from the follow

AppTheme.AppBarOverly and **AppTheme.PopupOverlay** may not inherit from one of the followings theme.

- 🔗android:style/Theme
- 🔗android:style/Theme.DeviceDefault
- 🔗android:style/Theme.Material

ny...@ukr.net <ny...@ukr.net> #27

#26, please investigate the code example in #19, too. It contains no overlays or bars, and uses system defaults rather than defining its own theme. When running in the Android 11 emulator i