App crashes with Fatal signal 5 (SIGTRAP)

+1 1 Hotlists Mark as Duplicate

Comments (3) Dependencies Duplicates (0) Blocking (0) Resources (1)

Fixed Bug P3 + Add Hotlist

STATUS UPDATE No update yet. Edit

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

Component used: androidx.browser

Version used: 1.3.0

Devices/Android versions reproduced on:

- Device: Xperia 5 II
- Android 11
- Android System Web View 94.0.4606.80
- Google Chrome 94.0.4606.80

When you open the new registration screen or password reset screen with CustomTabs and focus on the password entry field, Google Password Manager will be displayed. Then tap outside Goo

It is easy to reproduce if you clear all the tasks and operate.

If you open a web link in the Gmail app and do the same, it will crash too.

Logcat

```
2021-10-12 16:19:42.240 3220-30755/? E/NetworkScheduler.ATC: Called cancelTask for already completed task com.google.android.gms/.measurement.PackageMeasurem
2021-10-12 16:19:43.057 22917-22917/? A/chromium: [FATAL:jni_android.cc(306)] Please include Java exception stack in crash report
2021-10-12 16:19:43.164 3220-30755/? E/NetworkScheduler.ATC: Called cancelTask for already completed task com.google.android.gms/.measurement.PackageMeasurem
2021-10-12 16:19:43.225 31066-31066/? E/chromium: [1012/161943.225605:ERROR:process_memory_range.cc(75)] read out of range
2021-10-12 16:19:43.239 22917-22917/? A/libc: Fatal signal 5 (SIGTRAP), code -6 (SI_TKILL) in tid 22917 (.android.chrome), pid 22917 (.android.chrome)
2021-10-12 16:19:43.288 31069-31069/? A/DEBUG: *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
2021-10-12 16:19:43.288 31069-31069/? A/DEBUG: Build fingerprint: 'Sony/XQ-AS42/XQ-AS42:11/58.1.A.5.330/058001A005033003177046992:user/release-keys'
2021-10-12 16:19:43.288 31069-31069/? A/DEBUG: Revision: '0'
2021-10-12 16:19:43.288 31069-31069/? A/DEBUG: ABI: 'arm64'
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG: Timestamp: 2021-10-12 16:19:43+0900
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG: pid: 22917, tid: 22917, name: .android.chrome  >>> com.android.chrome <<<
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG: uid: 10320
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG: signal 5 (SIGTRAP), code -6 (SI_TKILL), fault addr --------
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG: Abort message: '[FATAL:jni_android.cc(306)] Please include Java exception stack in crash report
    '

2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     x0  0000000000000000  x1  0000007a4ccc7ac7  x2  ffffffffffffffff  x3  ffffffffffffffff
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     x4  0000000000000058  x5  b2feff7b3740cfc7  x6  b2feff7b3740cfc7  x7  ff7f7f7f7f7fffff
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     x8  0000000000000000  x9  0000000000000000  x10 0000000000000001  x11 0000000000000000
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     x12 00000000ffffff80  x13 0000000000000051  x14 000340e80efb049d  x15 0000000034155555
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     x16 0000007a52d61b08  x17 0000007db8739fdc  x18 0000007dbe86a000  x19 0000007fdb8be4c8
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     x20 0000007fdb8be4d8  x21 000000000000004f  x22 0000007db8744e80  x23 0000007a52d7a000
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     x24 0000007a52d7f0c8  x25 0000000000000000  x26 0000007dbdb12000  x27 0000007a52d7b000
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     x28 00000004000c8808  x29 0000007fdb8be460
2021-10-12 16:19:43.289 31069-31069/? A/DEBUG:     lr  0000007a4fdb2850  sp  0000007fdb8be010  pc  0000007a4fdb2988  pst 0000000060001000
2021-10-12 16:19:43.311 3220-22968/? E/NetworkScheduler.ATC: Called cancelTask for already completed task com.google.android.gms/.measurement.PackageMeasurem
2021-10-12 16:19:43.352 3798-21701/? E/FA-SVC: Task exception on worker thread: java.lang.IndexOutOfBoundsException: Index:2, Size:2
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG: backtrace:
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #00 pc 00000000033fd988  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #01 pc 0000000003477970  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #02 pc 0000000001b19d7c  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #03 pc 0000000005dcaaf4  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #04 pc 0000000005cfc6c4  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #05 pc 0000000005cfc488  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #06 pc 0000000005c04f90  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #07 pc 00000000028c1a48  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #08 pc 000000000369082c  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #09 pc 0000000003693514  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #10 pc 0000000003691828  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #11 pc 00000000038085c8  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #12 pc 0000000003692610  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #13 pc 0000000003431c18  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #14 pc 0000000003440084  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #15 pc 000000000346d938  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #16 pc 000000000346d8ec  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #17 pc 000000000346d6ac  /data/app/~~zZwXBwWcQJ_FwBnbjTrU5Q==/com.google.android.trichromelibrary_460608
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #18 pc 0000000000019da8  /system/lib64/libutils.so (android::Looper::pollInner(int)+916) (BuildId: 4e69b
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #19 pc 00000000000199ac  /system/lib64/libutils.so (android::Looper::pollOnce(int, int*, int*, void**)+1
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #20 pc 0000000000112b40  /system/lib64/libandroid_runtime.so (android::android_os_MessageQueue_nativePol
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #21 pc 0000000000210adc  /system/framework/arm64/boot-framework.oat (art_jni_trampoline+140) (BuildId: a
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #22 pc 000000000063f670  /system/framework/arm64/boot-framework.oat (android.os.MessageQueue.next+192) (
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #23 pc 000000000063b81c  /system/framework/arm64/boot-framework.oat (android.os.Looper.loop+812) (BuildI
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #24 pc 00000000003fdff0  /system/framework/arm64/boot-framework.oat (android.app.ActivityThread.main+752
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #25 pc 00000000001337e8  /apex/com.android.art/lib64/libart.so (art_quick_invoke_static_stub+568) (Build
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #26 pc 00000000001a8a94  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, uns
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #27 pc 0000000000555738  /apex/com.android.art/lib64/libart.so (art::InvokeMethod(art::ScopedObjectAcces
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #28 pc 00000000004d4ec4  /apex/com.android.art/lib64/libart.so (art::Method_invoke(_JNIEnv*, _jobject*,
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #29 pc 00000000000896f4  /apex/com.android.art/javalib/arm64/boot.oat (art_jni_trampoline+180) (BuildId:
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #30 pc 0000000000890eb8  /system/framework/arm64/boot-framework.oat (com.android.internal.os.RuntimeInit
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #31 pc 00000000008995e8  /system/framework/arm64/boot-framework.oat (com.android.internal.os.ZygoteInit.
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #32 pc 00000000001337e8  /apex/com.android.art/lib64/libart.so (art_quick_invoke_static_stub+568) (Build
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #33 pc 00000000001a8a94  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, uns
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #34 pc 0000000000554174  /apex/com.android.art/lib64/libart.so (art::JValue art::InvokeWithVarArgs<art::
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #35 pc 0000000000554628  /apex/com.android.art/lib64/libart.so (art::JValue art::InvokeWithVarArgs<_jmet
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #36 pc 0000000000438adc  /apex/com.android.art/lib64/libart.so (art::JNI<true>::CallStaticVoidMethodV(_J
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #37 pc 000000000009a424  /system/lib64/libandroid_runtime.so (_JNIEnv::CallStaticVoidMethod(_jclass*, _j
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #38 pc 00000000000a2260  /system/lib64/libandroid_runtime.so (android::AndroidRuntime::start(char const*
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #39 pc 0000000000003674  /system/bin/app_process64 (main+1580) (BuildId: f0690d7ea4979aa08ecaaff244e0498
2021-10-12 16:19:43.353 31069-31069/? A/DEBUG:       #40 pc 00000000000499e4  /apex/com.android.runtime/lib64/bionic/libc.so (__libc_init+108) (BuildId: 8d77
```

✓ **Links (1)**

Links (1)

“This is a Chrome bug that should be fixed with https://chromium-review.googlesource.com/c/chromium/src/+/3214744/ .”

COMMENTS

de...@gmail.com <de...@gmail.com> #2

We have an app, that uses the browser to login the user at our identity provider. Sadly chrome crashes at the latest version (Google Chrome 94.0.4606.80), so our users cannot login anymore

Any suggestions/help appreciated

```
10-12 11:21:12.122 10046 11328 11328 W System.err: Caused by: android.view.InflateException: Binary XML file line #6: Error inflating class org.chromium.c
10-12 11:21:12.128 10059 17008 17112 I ShortcutsDataManager: AbstractContentDataManager$ImportContentTask.doInBackground():249 doInBackground()
10-12 11:21:12.129 10059 17008 17112 I PersonalDictionaryDataHandler: PersonalDictionaryDataHandler.beginProcess():111 LanguageTags = [de]
10-12 11:21:12.132 10046 11328 11328 W System.err: Caused by: java.lang.reflect.InvocationTargetException
10-12 11:21:12.133 10046 11328 11328 W System.err:     at java.lang.reflect.Constructor.newInstance0(Native Method)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at java.lang.reflect.Constructor.newInstance(Constructor.java:343)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.createView(LayoutInflater.java:647)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.createViewFromTag(LayoutInflater.java:790)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.parseInclude(LayoutInflater.java:965)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.rInflate(LayoutInflater.java:859)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.rInflateChildren(LayoutInflater.java:824)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.rInflate(LayoutInflater.java:866)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.rInflateChildren(LayoutInflater.java:824)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.inflate(LayoutInflater.java:515)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.LayoutInflater.inflate(LayoutInflater.java:423)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.ViewStub.inflateViewNoAdd(ViewStub.java:269)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.view.ViewStub.inflate(ViewStub.java:302)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at Rz0.b(chromium-Monochrome.aab-stable-460608023:1)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at nP1.c(chromium-Monochrome.aab-stable-460608023:8)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at YR2.b(chromium-Monochrome.aab-stable-460608023:2)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at RR2.j(chromium-Monochrome.aab-stable-460608023:6)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at I02.c(chromium-Monochrome.aab-stable-460608023:40)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at YR2.b(chromium-Monochrome.aab-stable-460608023:2)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at RR2.l(chromium-Monochrome.aab-stable-460608023:6)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at I02.c(chromium-Monochrome.aab-stable-460608023:18)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at YR2.b(chromium-Monochrome.aab-stable-460608023:2)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at RR2.l(chromium-Monochrome.aab-stable-460608023:6)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at org.chromium.chrome.browser.keyboard_accessory.ManualFillingComponentBridge.showWhenKeyboardIsVi
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.os.MessageQueue.nativePollOnce(Native Method)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.os.MessageQueue.next(MessageQueue.java:326)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.os.Looper.loop(Looper.java:160)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at android.app.ActivityThread.main(ActivityThread.java:6863)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at java.lang.reflect.Method.invoke(Native Method)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run(RuntimeInit.java:537)
10-12 11:21:12.133 10046 11328 11328 W System.err:     at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:858)
10-12 11:21:12.134 10046 11328 11328 W System.err: Caused by: java.lang.UnsupportedOperationException: Failed to resolve attribute at index 24: TypedValue
10-12 11:21:12.134 10046 11328 11328 W System.err:     at android.content.res.TypedArray.getColorStateList(TypedArray.java:565)
10-12 11:21:12.134 10046 11328 11328 W System.err:     at 012.b(chromium-Monochrome.aab-stable-460608023:4)
10-12 11:21:12.134 10046 11328 11328 W System.err:     at com.google.android.material.tabs.TabLayout.<init>(chromium-Monochrome.aab-stable-460608023:58)
10-12 11:21:12.134 10046 11328 11328 W System.err:     at org.chromium.chrome.browser.keyboard_accessory.tab_layout_component.KeyboardAccessoryTabLayoutVi
10-12 11:21:12.134 10046 11328 11328 W System.err:     ... 31 more
10-12 11:21:12.139 10046 11328 11328 F chromium: [FATAL:jni_android.cc(306)] Please include Java exception stack in crash report
```

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

Marked as fixed.

This is a Chrome bug that should be fixed with https://chromium-review.googlesource.com/c/chromium/src/+/3214744/ .

It should be fixed in Chrome 94.0.4606.85.