

 Android Public Tracker > Framework 71421054 ▾


  ☆


UI crashed after some operations on the Settings application on hikey board with android-8.1.0_r2 tag

+1¹

Hotlists (2)

Mark as Duplicate





Comments (17)

Dependencies

Duplicates (0)

Blocking (0)

Resources (31)


Fixed

Bug

P3


+ Add Hotlist

[AOSP] assigned


 STATUS UPDATE

No update yet.

Edit

 DESCRIPTION

yo...@linaro.org created issue [#1](#)

Dec 29, 2017 10:50PM 

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

- Steps to reproduce the problem (including sample code if appropriate).

```
repo init -u https://android.googlesource.com/platform/manifest -m default.xml -b android-8.1.0_r2 -g default,device,notdefault,darwin,mips,x86 -p linux
repo sync -j32
pushd frameworks/native
git cherry-pick c9d2db18d8154ef527dbf4d34c7bb3317bbdc98c
popd
source build/envsetup.sh
lunch hikey-userdebug
make droidcore -j32 showcommands 2>&1 |tee build-hikey.log
```


- What happened.


After opened the settings application, and some clicks on the items there, the UI will be crashed.


Sometimes, the UI will be crashed(rebooted) after a while even without any manual operation on the UI after the home screen displayed.

- What you think the correct behavior should be.

There should be no UI crash happened, if some dialog popped up if there is any service or application errors

 deleted


0 B 

 Restricted

✓ Mentioned issues (3)

✓ Links (21)


Hide all

 Mentioned issues (3)

-- -- "I've opened an internal bug against ART here: b/71750393 (I can't just move this bug to the ART component, as it would remove public users from this issue)."rp...@ [#4](#), yo...@ [#14](#)

-- -- "<https://issuetracker.google.com/70631114>" yo...@ [#14](#)

-- -- "<https://issuetracker.google.com/71422357>" yo...@ [#14](#)

 Links (21)

"repo init -u <https://android.googlesource.com/platform/manifest> -m default.xml -b android-8.1.0_r2 -g default,device,notdefault,darwin,mips,x86 -p linux" yo...@ [#1](#)

"BTW, here is a similar problem: <https://github.com/facebook/fresco/issues/1885> , but not failed at the call of ucnv_close" yo...@ [#3](#)

"https://android.googlesource.com/platform/external/icu/+android-8.1.0_r7/icu4c/sourc... " yo...@ [#5](#)

"<https://android-review.googlesource.com/c/platform/libcore/+546505> Add size check in NativeConverter JNI code" yo...@ [#6](#)


"<https://android-review.googlesource.com/c/platform/libcore/+438439> Fix clang static analyzer warning in libcore" yo...@ [#6](#)


See all related links

COMMENTS

All comments ▾


↓ Oldest first


 ar...@google.com <ar...@google.com> [#2](#)

Dec 30, 2017 12:05AM 

Assigned to ar...@google.com.

Thank you for reporting this issue. We have shared this with our engineering team and will update this issue with more information as it becomes available.


 yo...@linaro.org <yo...@linaro.org> [#3](#)


Jan 9, 2018 07:32PM 


With some changes on luni/src/main/java/libcore/util/NativeAllocationRegistry.java, I am not able to reproduce the UI problem, but the change is obviously not right, it only makes the referent not garbage collected, so that the freeFunction is not called I think.

It looks like related to ./luni/src/main/java/java/nio/charset/CharsetEncoderICU.java,but still not able to find the root cause yet.

BTW, here is a similar problem: <https://github.com/facebook/fresco/issues/1885>, but not failed at the call of ucnv_close

 deleted

0 B 

 Restricted

rp...@google.com <rp...@google.com> [#4](#)

Jan 10, 2018 05:22AM

This looks like an ART GC bug.

I've opened an internal bug against ART here: [b/71750393](#) (I can't just move this bug to the ART component, as it would remove public users from this issue).

yo...@linaro.org <yo...@linaro.org> [#5](#)

Jan 11, 2018 02:03AM

with some hackings, I found that the crash is happened here in ucnv_close function:

https://android.googlesource.com/platform/external/icu/+android-8.1.0_r7/icu4c/source/common/ucnv.c#382

Like the following information I printed,

```
01-01 00:06:50.354 2949 2956 I System.out: LIUYQ libcore/luni/src/main/java/libcore/util/NativeAllocationRegistry.java CleanerThunk:
referent=java.nio.charset.CharsetEncoderICU@dee0a2b, nativePtr=499272083264, CleanerThunk=libcore.util.NativeAllocationRegistry$CleanerThunk@b105d74,
freeFunction=499167588800, size=200
01-01 00:06:50.354 2949 2956 E NativeConverter: ==LIUYQ == =libcore/luni/src/main/native/libcore_icu_NativeConverter.cpp:677 FreeNativeConverter 0x743eef6740
01-01 00:06:50.354 2949 2956 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv.c:357 ucnv_close_58 close converter UTF-8 at 0x743eef6740, isCopyLocal=0
01-01 00:06:50.354 2949 2956 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv.c:401 ucnv_close_58 close converter UTF-8 at 0x743eef6740, converter-
>subChars=0x5edc659c2c, converter->subUChars=0x743eef67c8
01-01 00:06:50.354 2949 2956 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv.c:406 ucnv_close_58 close converter UTF-8 at 0x743eef6740, it is allocated with
UCNV_ERROR_BUFFER_LENGTH * U_SIZEOF_UCHAR bytes
```

The addresses of converter->subChars and converter->subUChars are not the same, this causes the crash problem finally, but I could not find why the address of converter->subChars is changed to be different with converter->subUChars, they should be the same. and I do not find the the functions whichs change the address of converter->subChars get called.

Is it possible that some thing in the art heap management system or gc part that causes the address of converter->subChars changed?

yo...@linaro.org <yo...@linaro.org> [#6](#)

Jan 11, 2018 02:08AM

btw, I got the above hack information with following two changes cherry picked from master:

<https://android-review.googlesource.com/c/platform/libcore/+546505> Add size check in NativeConverter JNI code

<https://android-review.googlesource.com/c/platform/libcore/+438439> Fix clang static analyzer warning in libcore

rp...@google.com <rp...@google.com> [#7](#)

Jan 19, 2018 10:52PM

A tentative fix has been merged into AOSP (<https://android-review.googlesource.com/588293>). Yongqin, could you try to reproduce the issue with an AOSP top-of-the-tree build?

yo...@linaro.org <yo...@linaro.org> [#8](#)

Jan 20, 2018 04:46AM

Hi,
I am not able to reproduce it from master with hikey build, both before this change and after it.
but with change (<https://android-review.googlesource.com/588293>) applied on android-8.1.0_r7 tag, the problem still could be reproduced with hikey.

And another thing I found that, with this change(<https://android-review.googlesource.com/c/device/linaro/hikey/+471999/1>) cherry picked, the 8.1 build could not be booted up to home screen, and the log is the same related to ucnv_close problem, it seems that the change(<https://android-review.googlesource.com/c/device/linaro/hikey/+471999/1>) makes this problem happen more easily.

be...@gmail.com <be...@gmail.com> [#9](#)

Jan 20, 2018 11:11AM

Change 471999 essentially makes /sys/kernel/debug readable -- making it rather likely that the problem is triggered by an attempt to log an error that happened elsewhere (and that simply isn't being detected because of debugfs not being readable).

Makes me wonder if it's reproducible in -user (as opposed to -eng and -userdebug) builds...

yo...@linaro.org <yo...@linaro.org> [#10](#)

Jan 21, 2018 01:22AM

Tried with user build. but since there is adb connection and serial console shell enabled by default, and usb otg and usb host could not be enabled at the same time. I am not able to check the logcat information, but there are UI crash problem happend with the user build too.

yo...@linaro.org <yo...@linaro.org> [#11](#)

Jan 23, 2018 12:04AM

With some hackings, found that the UConverter which causes crash problem is allocated from the call of android.util.Slog.wtf, the line here: https://android.googlesource.com/platform/frameworks/base/+android-8.1.0_r7/core/java/com/android/internal/os/KernelWakelockReader.java#82,

Like the log following, but could not find any obvious message from the log.

And if I applied the change(<https://android-review.googlesource.com/c/device/linaro/hikey/+471999/1>) to make /sys/kernel/debug readable, it will cause the build failed to boot up to home screen.

```
01-21 17:17:28.214 1000 2009 2028 E System : LIUYQ NativeConverter.registerConverterp
CharsetEncoderICU=java.nio.charset.CharsetEncoderICU@56ed74a converterHandle=0x78580f6600
01-21 17:17:28.215 1000 2009 2028 E System : java.lang.Error: LIUYQ NativeConverter.registerConverterp
CharsetEncoderICU=java.nio.charset.CharsetEncoderICU@56ed74a converterHandle=0x78580f6600
01-21 17:17:28.215 1000 2009 2028 E System :
01-21 17:17:28.215 1000 2009 2028 E System : at libcore.icu.NativeConverter.registerConverter(NativeConverter.java:34)
```

```

01-21 17:17:28.215 1000 2009 2028 E System : at java.nio.charset.CharsetEncoder$ICU.newInstance(CharsetEncoder$ICU.java:84)
01-21 17:17:28.215 1000 2009 2028 E System : at java.nio.charset.Charset$ICU.newEncoder(Charset$ICU.java:27)
01-21 17:17:28.215 1000 2009 2028 E System : at com.android.internal.util.FastPrintWriter.initDefaultEncoder(FastPrintWriter.java:292)
01-21 17:17:28.215 1000 2009 2028 E System : at com.android.internal.util.FastPrintWriter.<init>(FastPrintWriter.java:201)
01-21 17:17:28.215 1000 2009 2028 E System : at android.app.ApplicationErrorReport$CrashInfo.<init>(ApplicationErrorReport.java:346)
01-21 17:17:28.215 1000 2009 2028 E System : at android.app.ApplicationErrorReport$ParcelableCrashInfo.<init>(ApplicationErrorReport.java:475)
01-21 17:17:28.215 1000 2009 2028 E System : at com.android.internal.os.RuntimeInit.wtf(RuntimeInit.java:334)
01-21 17:17:28.215 1000 2009 2028 E System : at android.util.Log$1.onTerribleFailure(Log.java:110)
01-21 17:17:28.215 1000 2009 2028 E System : at android.util.Log.wtf(Log.java:304)
01-21 17:17:28.215 1000 2009 2028 E System : at android.util.Slog.wtf(Slog.java:82)
01-21 17:17:28.215 1000 2009 2028 E System : at com.android.internal.os.KernelWakelockReader.readKernelWakelockStats(KernelWakelockReader.java:94)
01-21 17:17:28.215 1000 2009 2028 E System : at com.android.internal.os.BatteryStatsImpl.updateKernelWakelocksLocked(BatteryStatsImpl.java:10380)
01-21 17:17:28.215 1000 2009 2028 E System : at com.android.server.am.BatteryExternalStatsWorker.updateExternalStatsLocked(BatteryExternalStatsWorker.java:263)
01-21 17:17:28.215 1000 2009 2028 E System : at com.android.server.am.BatteryExternalStatsWorker.-wrap0(Unknown Source:0)
01-21 17:17:28.215 1000 2009 2028 E System : at com.android.server.am.BatteryExternalStatsWorker$1.run(BatteryExternalStatsWorker.java:180)
01-21 17:17:28.215 1000 2009 2028 E System : at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:457)
01-21 17:17:28.215 1000 2009 2028 E System : at java.util.concurrent.FutureTask.run(FutureTask.java:266)
01-21 17:17:28.215 1000 2009 2028 E System : at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1162)
01-21 17:17:28.215 1000 2009 2028 E System : at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:636)
01-21 17:17:28.215 1000 2009 2028 E System : at java.lang.Thread.run(Thread.java:764)

01-21 17:17:29.988 1000 2009 2016 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv.c:356 ucnv_close_58 close converter at 0x78580f6600, converter-
>sharedData=0x78da4f1d58
01-21 17:17:29.988 1000 2009 2016 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv.c:357 ucnv_close_58 close converter at 0x78580f6600, converter-
>subChars=0x2158ab5819, converter->subUChars=0x78580f6688, converter->subCharLen=3, converter->fromUContext=0x784d0cee00, converter->toUContext=0x0, converter-
>fromUCharErrorBehaviour=0x7851e89fc4, converter->fromCharErrorBehaviour=0x78da3d5e18
01-21 17:17:29.988 1000 2009 2016 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv.c:401 ucnv_close_58 close converter UTF-8 at 0x78580f6600, converter-
>subChars=0x2158ab5819, converter->subUChars=0x78580f6688, converter->subCharLen=3
01-21 17:17:29.989 1000 2009 2016 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv.c:406 ucnv_close_58 close converter UTF-8 at 0x78580f6600, converter-
>subChars=0x2158ab5819, converter->subUChars=0x78580f6688, converter->subCharLen=3

01-21 17:17:29.989 1000 2009 2016 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv.c:406 ucnv_close_58 close converter UTF-8 at 0x78580f6600, converter-
>subChars=0x2158ab5819, converter->subUChars=0x78580f6688, converter->subCharLen=3
----- beginning of crash
01-21 17:17:29.990 1000 2009 2016 F libc : Fatal signal 11 (SIGSEGV), code 1, fault addr 0x2158a005b8 in tid 2016 (ReferenceQueueD), pid 2009 (system_server)
01-21 17:17:30.150 1000 2842 2842 I crash_dump64: obtaining output fd from tombstoned, type: kDebuggerdTombstone
01-21 17:17:30.151 1058 1914 1914 I /system/bin/tombstoned: received crash request for pid 2009
01-21 17:17:30.155 1000 2842 2842 I crash_dump64: performing dump of process 2009 (target tid = 2016)
01-21 17:17:30.156 1000 2842 2842 F DEBUG : *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
01-21 17:17:30.157 1000 2842 2842 F DEBUG : Build fingerprint: 'Android/hikey/hikey:8.1.0/OPM3.171019.013/liu01202124:userdebug/test-keys'
01-21 17:17:30.157 1000 2842 2842 F DEBUG : Revision: '0'
01-21 17:17:30.157 1000 2842 2842 F DEBUG : ABI: 'arm64'
01-21 17:17:30.157 1000 2842 2842 F DEBUG : pid: 2009, tid: 2016, name: ReferenceQueueD >>> system_server <<<
01-21 17:17:30.157 1000 2842 2842 F DEBUG : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x2158a005b8
01-21 17:17:30.157 1000 2842 2842 F DEBUG : x0 000000784d113288 x1 0000002158ab5819 x2 000000785805cc00 x3 0000000000000000
01-21 17:17:30.157 1000 2842 2842 F DEBUG : x4 003d000000000000 x5 0080000000000000 x6 0900000000000000 x7 0000000000000809
01-21 17:17:30.157 1000 2842 2842 F DEBUG : x8 0000002158a00540 x9 00000000000000a8 x10 00000000000000b5 x11 00000000000000cb
01-21 17:17:30.157 1000 2842 2842 F DEBUG : x12 000000784d56a968 x13 0000000000000003 x14 ffffffff x15 0900000000000000
01-21 17:17:30.157 1000 2842 2842 F DEBUG : x16 00000078dc491ca8 x17 00000078dc42e4b8 x18 0000000000000008 x19 0000002158ab5819
01-21 17:17:30.158 1000 2842 2842 F DEBUG : x20 000000784d113288 x21 000000785805cc00 x22 0000000000000000 x23 00000078dc49c8b8
01-21 17:17:30.158 1000 2842 2842 F DEBUG : x24 00000078dc49c934 x25 0000000013ca3f20 x26 000000785806e2a0 x27 0000000000000001
01-21 17:17:30.158 1000 2842 2842 F DEBUG : x28 000000784d56b588 x29 000000784d56ad20 x30 00000078dc45a8b8
01-21 17:17:30.158 1000 2842 2842 F DEBUG : sp 000000784d56acf0 pc 00000078dc45a364 pstate 0000000080000000
01-21 17:17:30.216 1000 1888 2519 W GrallocMapperPassthrough: buffer descriptor with invalid usage bits 0x400
01-21 17:17:30.431 1000 2842 2842 F DEBUG :
01-21 17:17:30.431 1000 2842 2842 F DEBUG : backtrace:
01-21 17:17:30.431 1000 2842 2842 F DEBUG : #00 pc 00000000000094364 /system/lib64/libc.so (ifree+88)
01-21 17:17:30.431 1000 2842 2842 F DEBUG : #01 pc 000000000000948b4 /system/lib64/libc.so (je_free+120)
01-21 17:17:30.431 1000 2842 2842 F DEBUG : #02 pc 0000000000007dbf8 /system/lib64/libicuuc.so (ucnv_close_58+668)
01-21 17:17:30.431 1000 2842 2842 F DEBUG : #03 pc 00000000002e8de0 /system/framework/arm64/boot-core-libart.oat (offset 0xd5000) (java.math.NativeBN.BN_copy
[DEDUPED]+160)
01-21 17:17:30.431 1000 2842 2842 F DEBUG : #04 pc 000000000032020c /system/framework/arm64/boot-core-libart.oat (offset 0xd5000)
(libcore.util.NativeAllocationRegistry$CleanerThunk.run+76)
01-21 17:17:30.431 1000 2842 2842 F DEBUG : #05 pc 00000000006ab8c4 /system/framework/arm64/boot.oat (offset 0x1da000) (sun.misc.Cleaner.clean+132)
01-21 17:17:30.431 1000 2842 2842 F DEBUG : #06 pc 00000000002dd6fc /system/framework/arm64/boot.oat (offset 0x1da000)
(java.lang.ref.ReferenceQueue.enqueueLocked+252)
01-21 17:17:30.431 1000 2842 2842 F DEBUG : #07 pc 00000000002dd81c /system/framework/arm64/boot.oat (offset 0x1da000)
(java.lang.ref.ReferenceQueue.enqueuePending+172)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #08 pc 00000000002cbf28 /system/framework/arm64/boot-core-libart.oat (offset 0xd5000)
(java.lang.Daemons$ReferenceQueueDaemon.runInternal+248)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #09 pc 00000000002ca6dc /system/framework/arm64/boot-core-libart.oat (offset 0xd5000)
(java.lang.Daemons$Daemon.run+76)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #10 pc 00000000001f97b8 /system/framework/arm64/boot.oat (offset 0x1da000) (java.lang.Thread.run+72)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #11 pc 000000000054ab88 /system/lib64/libart.so (art_quick_invoke_stub+584)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #12 pc 00000000000dc594 /system/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*,
char const*)+204)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #13 pc 000000000046edc8 /system/lib64/libart.so (art::InvokeWithArgArray(art::ScopedObjectAccessAlreadyRunnable const&,
art::ArtMethod*, art::ArgArray*, art::JValue*, char const*)+100)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #14 pc 0000000000470008 /system/lib64/libart.so
(art::InvokeVirtualOrInterfaceWithJValues(art::ScopedObjectAccessAlreadyRunnable const&, _jobject*, _jmethodID*, jvalue*)+836)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #15 pc 0000000000496ab4 /system/lib64/libart.so (art::Thread::CreateCallback(void*)+1120)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #16 pc 0000000000067d0c /system/lib64/libc.so (__pthread_start(void*)+36)
01-21 17:17:30.432 1000 2842 2842 F DEBUG : #17 pc 000000000001eba4 /system/lib64/libc.so (__start_thread+68)

```

yo...@linaro.org <yo...@linaro.org> #12

Jan 23, 2018 12:10AM ⋮

Another strange thing is that, the allocated Converter could be at the same address for multiple times.
Like from the bugreport-8.1-icu.zip attached before:

```
21:07:53 liu: work$ grep 'ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at 0x78580f6d80,' bugreport-hikey-OPM3.171019.013-2018-01-21-17-17-59.txt
01-21 17:15:25.629 1000 2009 2034 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:15:26.450 1000 2009 2009 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:15:27.175 1000 2009 2009 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:15:27.709 1000 2009 2009 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:15:28.516 1000 2009 2009 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:15:28.583 10049 2124 2314 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:15:29.897 1000 2009 2228 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:15:32.491 1000 2009 2483 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:15:34.228 1000 2009 2267 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
01-21 17:16:32.928 1000 2009 2083 E UCNV.C : ==LIUYQ == =external/icu/icu4c/source/common/ucnv_bld.cpp:1028 ucnv_createConverterFromSharedData_58 ucnv_open UTF-8 at
0x78580f6d80, converter->subChars=0x78580f6e08, converter->subUChars=0x78580f6e08
21:08:12 liu: work$
```

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

Jan 23, 2018 04:57AM ⋮

It would be good to understand whether this is fixed by <https://android-review.googlesource.com/c/platform/libcore/+588293> . That CL should only matter in out-of-memory situations.

yo...@linaro.org <yo...@linaro.org> #14

Jan 23, 2018 05:10AM ⋮

On 23 January 2018 at 01:57, <buganizer-system@google.com> wrote:

- Show quoted text -

No, after applied the change <https://android-review.googlesource.com/c/platform/libcore/+588293>
<<https://www.google.com/url?q=https://android-review.googlesource.com/c/platform/libcore/%2B/588293&sa=D&usq=AFQjCNH78A5PtWD4etpD8OHullilpNxxkg>>
,

the problem still could be reproduced on hikey with the android-8.1.0_r7 tag.

The attchement bugreport-8.1-icu.zip attached was captured with change 588293

<<https://www.google.com/url?q=https://android-review.googlesource.com/c/platform/libcore/%2B/588293&sa=D&usq=AFQjCNH78A5PtWD4etpD8OHullilpNxxkg>>
applied.

BTW, now I am using following monkey command to reproduce the problem:
adb shell monkey -s 3 -pct-syskeys 0 -p com.android.settings 10000

Thanks,
Yongqin Liu

- Show quoted text -

Best Regards,
Yongqin Liu

#mailing list
linaro-android@lists.linaro.org <linaro-dev@lists.linaro.org>
<http://lists.linaro.org/mailman/listinfo/linaro-android>

hb...@google.com <hb...@google.com>

Feb 7, 2018 04:14AM

Reassigned to hb...@google.com.

yo...@linaro.org <yo...@linaro.org> #15

Mar 5, 2018 02:33PM ⋮

I do not know the reason, but change like this seems help to make this problem happen less.
https://android-review.linaro.org/#/c/18093/1/icu4c/source/common/ucnv_bld.h

Especially it could help to make the build booted up to home screen after has the debugfs readable for others(the change here applied <https://android->

[review.googlesource.com/c/device/linaro/hikey/+471999/1](https://android-review.googlesource.com/c/device/linaro/hikey/+471999/1)).

Otherwise it could not boot up to home screen after the change <https://android-review.googlesource.com/c/device/linaro/hikey/+471999/1> applied.

And I also tried with following 3 changes applied, but they do not help much on this problem.:(

Fix clang static analyzer warning in libcore:

<https://android.googlesource.com/platform/libcore/+4bdd5651813b17dcd895eaac9bde911126287fa5%5E%21/>

Add size check in NativeConverter JNI code

<https://android.googlesource.com/platform/libcore/+fef459ae66f78b180f05942c9f659781c3822d07%5E!/#F0>

Avoid duplicate free in CharsetXcoderICU on OOME

<https://android.googlesource.com/platform/libcore/+59b140db4c4bd7617792256cd5d52713409137bc%5E!/#F0>

Add reachabilityFence, ReachabilitySensitive

<https://android.googlesource.com/platform/libcore/+e31b37859051d3902e06e4ba384995df7188917f%5E!/#F0>

Thanks,
Yongqin Liu



yo...@linaro.org <yo...@linaro.org> [#16](#)

Mar 10, 2018 06:32AM ⋮

This seems to be hikey specific problem, and the fix is here:

<https://android.googlesource.com/device/linaro/hikey/+5af9bdca62d686dd0554269f1ef4027e9a95b60b%5E%21/#F0>

but not understand why it always cause ucnv_close crash, in theory, the the corrupt memory should be random.



hb...@google.com <hb...@google.com> [#17](#)

May 10, 2018 07:23AM ⋮

Marked as fixed.

Closing, since the CL mentioned in #16 (<https://android-review.googlesource.com/c/device/linaro/hikey/+528739>) was merged long ago, and there doesn't seem to be any more discussion here. Please reopen if there is still an issue.