KeyCharacterMap::writeToParcel Native crash

+1 1 Hotlists (4) Mark as Duplicate

Comments (5) Dependencies Duplicates (0) Blocking (0) Resources (0)

Assigned Bug P3 + Add Hotlist [AOSP] assigned

STATUS UPDATE No update yet. Edit

DESCRIPTION wa...@lenovo.corp-partner.google.com created issue #1 Sep 14, 2023 10:00PM

We encountered a fatal exception in the use of the process, the system restarted, see the error in the Key Character Map :: write To Parcel, MTK provides us with a modification plan, here is pure native, please Google to help see if this patch is reasonable, thank you

```
The error stack is as follows:
Build fingerprint:
'Lenovo/TB132FU/TB132FU:13/TP1A.220624.014/TB132FU_S240207_230909_ROW:user/release-keys'
Revision: '0'
ABI: 'arm64'
Timestamp: 2023-09-11 15:04:03.400412864+0900
Process uptime: 4874s
Cmdline: system_server
pid: 1332, tid: 4857, name: binder:1332_B  >>> system_server <<<
uid: 1000
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x00666e6f632e6f7a
    x0  0000000000000000  x1  0000000000000001  x2  0000000000000021  x3  ffffffffffffffff
    x4  b400007d24918a71  x5  b400007d656919b1  x6  2f6d65747379732f  x7  6379656b2f727375
    x8  0000000000000064  x9  0000000000000060  x10 0000000000000001  x11 686379656b2f7273
    x12 656e65472f737261  x13 006d636b2e636972  x14 b400007ea3cdc980  x15 0000000000000003
    x16 0000007e9ed66ce0  x17 0000007e9253e750  x18 0000007ca421e000  x19 0000007cc3b79920
    x20 b400007dca04e640  x21 0000007e9ed209c5  x22 000000000000006d  x23 69666e6f632e6f72
    x24 0000000000000000  x25 0000007e9ed1e9e2  x26 0000007e9ed1fd7c  x27 b400007d655d7880
    x28 0000007cc3b79184  x29 0000007cc3b78fe0
    lr  0000007e9ed40ce0  sp  0000007cc3b78fe0  pc  0000007e9ed40ce0  pst 0000000020001000

backtrace:
      #00 pc 000000000003fce0  /system/lib64/libinput.so
(android::KeyCharacterMap::writeToParcel(android::Parcel*) const+272) (BuildId:
2b7e1da68a871b0dca3e2a15d3706524)
      #01 pc 000000000012f608  /system/lib64/libandroid_runtime.so (android::nativeWriteToParcel(_JNIEnv*,
_jobject*, long, _jobject*)+136) (BuildId: d49070f4cfea1bc7f9f03af489b6b073)
      #02 pc 00000000001d9bd4  /system/framework/arm64/boot-framework.oat (art_jni_trampoline+132)
(BuildId: cb40a22a5208fe9d69ff49fc7a4e59edfb028fec)
      #03 pc 0000000000209a9c  /apex/com.android.art/lib64/libart.so (nterp_helper+1948) (BuildId:
28c5aa8a2e8fc5df069f717d6e94f7fe)
      #04 pc 00000000003d475c  /system/framework/framework.jar
(android.view.KeyCharacterMap.writeToParcel+20)
      #05 pc 000000000206bf8c  /memfd:jit-cache (deleted) (android.view.InputDevice.writeToParcel+124)
      #06 pc 00000000005b641c  /system/framework/arm64/boot-framework.oat
(android.os.Parcel.writeTypedObject+140) (BuildId: cb40a22a5208fe9d69ff49fc7a4e59edfb028fec)
      #07 pc 00000000020a2bac  /memfd:jit-cache (deleted)
(android.hardware.input.IInputManager$Stub.onTransact+18844)
      #08 pc 00000000005f4618  /system/framework/arm64/boot-framework.oat
(android.os.Binder.execTransactInternal+744) (BuildId: cb40a22a5208fe9d69ff49fc7a4e59edfb028fec)
      #09 pc 00000000005f4210  /system/framework/arm64/boot-framework.oat
(android.os.Binder.execTransact+304) (BuildId: cb40a22a5208fe9d69ff49fc7a4e59edfb028fec)
      #10 pc 000000000043476c  /apex/com.android.art/lib64/libart.so (art_quick_invoke_stub+556) (BuildId:
28c5aa8a2e8fc5df069f717d6e94f7fe)
      #11 pc 00000000004c87e8  /apex/com.android.art/lib64/libart.so (art::JValue
art::InvokeVirtualOrInterfaceWithVarArgs<art::ArtMethod*>(art::ScopedObjectAccessAlreadyRunnable const&,
_jobject*, art::ArtMethod*, std::__va_list)+828) (BuildId: 28c5aa8a2e8fc5df069f717d6e94f7fe)
      #12 pc 00000000005d487c  /apex/com.android.art/lib64/libart.so
(art::JNI<false>::CallBooleanMethodV(_JNIEnv*, _jobject*, _jmethodID*, std::__va_list)+184) (BuildId:
28c5aa8a2e8fc5df069f717d6e94f7fe)
      #13 pc 00000000000c17b8  /system/lib64/libandroid_runtime.so (_JNIEnv::CallBooleanMethod(_jobject*,
_jmethodID*, ...)+120) (BuildId: d49070f4cfea1bc7f9f03af489b6b073)
      #14 pc 00000000001734cc  /system/lib64/libandroid_runtime.so (JavaBBinder::onTransact(unsigned int,
android::Parcel const&, android::Parcel*, unsigned int)+156) (BuildId: d49070f4cfea1bc7f9f03af489b6b073)
      #15 pc 0000000000050a4c  /system/lib64/libbinder.so (android::BBinder::transact(unsigned int,
android::Parcel const&, android::Parcel*, unsigned int)+236) (BuildId: 4db68b9b4fc78875c67e29b43bdfb2b0)
      #16 pc 000000000005bbcc  /system/lib64/libbinder.so
```

Reporter	○ wa...@lenovo.corp-partner.g...
Type	Bug
Priority	P3
Severity	S3
Status	Assigned
Access	Default access View
Assignee	○ vi...@google.com
Verifier	--
Collaborators	
CC	wa...@lenovo.corp-partner.google.
AOSP ID	--
ReportedBy	Developer
Found In	--
Targeted To	--
Verified In	--
In Prod	○

```
(android::IPCThreadState::executeCommand(int)+1036) (BuildId: 4db68b9b4fc78875c67e29b43bdfb2b0)
      #17 pc 000000000005b6f0  /system/lib64/libbinder.so
(android::IPCThreadState::getAndExecuteCommand()+160) (BuildId: 4db68b9b4fc78875c67e29b43bdfb2b0)
      #18 pc 000000000005c0c4  /system/lib64/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+68)
(BuildId: 4db68b9b4fc78875c67e29b43bdfb2b0)
      #19 pc 000000000008bf78  /system/lib64/libbinder.so (android::PoolThread::threadLoop()+24) (BuildId:
4db68b9b4fc78875c67e29b43bdfb2b0)
      #20 pc 0000000000013440  /system/lib64/libutils.so (android::Thread::_threadLoop(void*)+416) (BuildId:
10aac5d4a671e4110bc00c9b69d83d8a)
      #21 pc 00000000000c9fcc  /system/lib64/libandroid_runtime.so
(android::AndroidRuntime::javaThreadShell(void*)+140) (BuildId: d49070f4cfea1bc7f9f03af489b6b073)
      #22 pc 00000000000fad2c  /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+204)
(BuildId: 2583c9158302542a2277fbb874e281ce)
      #23 pc 000000000008e1b0  /apex/com.android.runtime/lib64/bionic/libc.so (__start_thread+64) (BuildId:
2583c9158302542a2277fbb874e281ce)
```

The patch is as follows:3f4450d.diff

deleted
0 B

Restricted

COMMENTS

All comments ▾   ↓ Oldest first

wa...@lenovo.corp-partner.google.com <wa...@lenovo.corp-partner.google.com> #2
Sep 14, 2023 10:01PM

hi google
please help me see if this patch is reasonable, thank you

vi...@google.com <vi...@google.com> #3
Sep 14, 2023 11:29PM

Assigned to vi...@google.com.

We have shared this with our product and engineering team and will update this issue with more information as it becomes available.

wa...@lenovo.corp-partner.google.com <wa...@lenovo.corp-partner.google.com> #4
Sep 18, 2023 01:19PM

hi google
any update?

wa...@lenovo.corp-partner.google.com <wa...@lenovo.corp-partner.google.com> #5
Sep 21, 2023 12:49PM

hi google
this issue occurred on machines on the Lenovo Android 13 platform. Is there any progress now?