Native Crash in system_server when DUT boot.

Fixed Bug P4 + Add Hotlist [AOSP] Released NeedsInfo

STATUS UPDATE No update yet. Edit

DESCRIPTION ji...@gmail.com created issue #1 Oct 29, 2015 06:36PM

It will not entering Android after Native Crash when DUT boot.
This is really serious problem.
Reproduce rate: very low. But not only once.

```
10-22 17:15:59.265 896 896 F libc : Fatal signal 7 (SIGBUS), code 2, fault addr 0x7f8ac65000 in tid 896 (system_server)
10-22 17:15:59.381 315 315 I DEBUG : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
10-22 17:15:59.381 315 315 I DEBUG : Revision: '0'
10-22 17:15:59.381 315 315 I DEBUG : ABI: 'arm64'
10-22 17:15:59.381 315 315 I DEBUG : pid: 896, tid: 896, name: system_server >>> system_server <<<
10-22 17:15:59.381 315 315 I DEBUG : signal 7 (SIGBUS), code 2 (BUS_ADRERR), fault addr 0x7f8ac65000
10-22 17:15:59.399 315 315 I DEBUG : x0 0000007f8ac64000 x1 0000007fdd984780 x2 0000000000006fb8 x3 0000000000000000
10-22 17:15:59.400 315 315 I DEBUG : x4 0000000000000008 x5 0000000000008000 x6 0000007f8ac64fb8 x7 0000332600090022
10-22 17:15:59.400 315 315 I DEBUG : x8 0000017c000ee589 x9 0000334500090012 x10 00000254000ed8bd x11 0000344700090022
10-22 17:15:59.400 315 315 I DEBUG : x12 000000cc000edb11 x13 0000322400090022 x14 00000254000ed8bd x15
0000000000000000
10-22 17:15:59.400 315 315 I DEBUG : x16 0000007fb0354e70 x17 0000007fb0967680 x18 0000000000008000 x19
0000000000008000
10-22 17:15:59.400 315 315 I DEBUG : x20 0000000000008000 x21 0000007fdd97b788 x22 0000000000000161 x23
0000007fdd97b790
10-22 17:15:59.400 315 315 I DEBUG : x24 0000007fdd983788 x25 0000000000008000 x26 000000000014e986 x27
0000000000008000
10-22 17:15:59.400 315 315 I DEBUG : x28 0000000000000000 x29 0000007fdd97b680 x30 0000007fb033538c
10-22 17:15:59.400 315 315 I DEBUG : sp 0000007fdd97b680 pc 0000007fb09677ac pstate 0000000020000000
10-22 17:15:59.401 315 315 I DEBUG :
10-22 17:15:59.401 315 315 I DEBUG : backtrace:
10-22 17:15:59.401 315 315 I DEBUG : #00 pc 00000000000137ac /system/lib64/libc.so (memcpy+300)
10-22 17:15:59.401 315 315 I DEBUG : #01 pc 000000000002e388 /system/lib64/libandroidfw.so
10-22 17:15:59.401 315 315 I DEBUG : #02 pc 000000000002f258 /system/lib64/libandroidfw.so (ExtractToMemory+328)
10-22 17:15:59.401 315 315 I DEBUG : #03 pc 000000000002f398 /system/lib64/libandroidfw.so (ExtractEntryToFile+268)
10-22 17:15:59.401 315 315 I DEBUG : #04 pc 00000000000285a8 /system/lib64/libandroidfw.so
(android::ZipFileRO::uncompressEntry(void*, int) const+12)
10-22 17:15:59.401 315 315 I DEBUG : #05 pc 000000000008f27c /system/lib64/libandroid_runtime.so
10-22 17:15:59.402 315 315 I DEBUG : #06 pc 000000000008f66c /system/lib64/libandroid_runtime.so
10-22 17:15:59.402 315 315 I DEBUG : #07 pc 000000000008f77c /system/lib64/libandroid_runtime.so
10-22 17:15:59.402 315 315 I DEBUG : #08 pc 0000000000378740 /system/framework/arm64/boot.oat

Back trace:
#00 0137ac /system/lib64/libc.so (memcpy+300)
memcpy
bionic/libc/arch-arm64/generic/bionic/memcpy.S:171
#01 02e388 /system/lib64/libandroidfw.so
_ZL13InflateToFileiPK8ZipEntryPhjPm.isra.0
system/core/libziparchive/zip_archive.cc:1081
#02 02f258 /system/lib64/libandroidfw.so (ExtractToMemory+328)
ExtractToMemory
system/core/libziparchive/zip_archive.cc:1105
#03 02f398 /system/lib64/libandroidfw.so (ExtractEntryToFile+268)
ExtractEntryToFile
system/core/include/utils/FileMap.h:91
#04 0285a8 /system/lib64/libandroidfw.so (android::ZipFileRO::uncompressEntry(void*, int) const+12)
android::ZipFileRO::uncompressEntry(void*, int) const
frameworks/base/libs/androidfw/ZipFileRO.cpp:257
#05 08f27c /system/lib64/libandroid_runtime.so
android::copyFileIfChanged(_JNIEnv*, void*, android::ZipFileRO*, void*, char const*)
frameworks/base/core/jni/com_android_internal_content_NativeLibraryHelper.cpp:248
#06 08f66c /system/lib64/libandroid_runtime.so
android::iterateOverNativeFiles(_JNIEnv*, long, _jstring*, android::install_status_t (*)(_JNIEnv*, void*, android::ZipFileRO*, void*, char
const*), void*)
libnativehelper/include/nativehelper/jni.h:851
#07 08f77c /system/lib64/libandroid_runtime.so
android::register_com_android_internal_content_NativeLibraryHelper(_JNIEnv*)
frameworks/base/core/jni/com_android_internal_content_NativeLibraryHelper.cpp:576
#08 378740 /system/framework/arm64/boot.oat
??:?
```

Links (4) Hide all

"http://b.ge" ji...@ #2

Reporter ji...@gmail.com
Type Bug
Priority P4
Severity S3
Status Fixed
Access Default access View
Assignee na...@google.com
Verifier --
Collaborators
CC
cf...@google.com
en...@google.com
ji...@gmail.com
jo...@sonymobile.com
na...@google.com
AOSP ID 191859
ReportedBy User
Found In --
Targeted To --
Verified In --
In Prod

“http://b.ne” ji...@ #2

“ …e http://developer.android.com/tools/help/logcat.html . Copy and paste relevant sections of the logcat output into this is… ” rn...@ #3

“We have seen this, yes. The fix for our problem was uploaded here: https://android-review.googlesource.com/#/c/146996/ .” jo...@ #10

COMMENTS

All comments ↓ Oldest first

ji...@gmail.com <ji...@gmail.com> #2 Oct 29, 2015 07:58PM

I found my codebase exist difference with AOSP codebase.

Here's backtrace in my codebase.

```
#00 0137ac /system/lib64/libc.so (memcpy+300)
   memcpy
   bionic/libc/arch-arm64/generic/bionic/memcpy.S:171

154        /* Critical loop.  Start at a new cache line boundary.  Assuming
155         * 64 bytes per line this ensures the entire loop is in one line.  */
156        .p2align 6
157 .Lcpy_body_large:
158        /* There are at least 128 bytes to copy.  */
159        ldp     A_l, A_h, [src, #0]
160        sub     dst, dst, #16          /* Pre-bias.  */
161        ldp     B_l, B_h, [src, #16]
162        ldp     C_l, C_h, [src, #32]
163        ldp     D_l, D_h, [src, #48]!   /* src += 64 - Pre-bias.  */
164 1:
165        stp     A_l, A_h, [dst, #16]
166        ldp     A_l, A_h, [src, #16]
167        stp     B_l, B_h, [dst, #32]
168        ldp     B_l, B_h, [src, #32]
169        stp     C_l, C_h, [dst, #48]
170        ldp     C_l, C_h, [src, #48]
171        stp     D_l, D_h, [dst, #64]!
172        ldp     D_l, D_h, [src, #64]!
173        subs    count, count, #64
174        b.ge    1b
175        stp     A_l, A_h, [dst, #16]
176        stp     B_l, B_h, [dst, #32]
177        stp     C_l, C_h, [dst, #48]
178        stp     D_l, D_h, [dst, #64]
179        add     src, src, #16
180        add     dst, dst, #64 + 16
181        tst     count, #0x3f
182        b.ne    .Ltail63
183        ret
184 END(memcpy)


#01 02e388 /system/lib64/libandroidfw.so
   _ZL13InflateToFileiPK8ZipEntryPhjPm.isra.0
   system/core/libziparchive/zip_archive.cc:1081
#02 02f258 /system/lib64/libandroidfw.so (ExtractToMemory+328)
   ExtractToMemory
   system/core/libziparchive/zip_archive.cc:1105

1078   assert(zerr == Z_STREAM_END);     /* other errors should've been caught */
1079
1080   // stream.adler holds the crc32 value for such streams.
1081   *crc_out = zstream.adler;
1082
1083   if (zstream.total_out != uncompressed_length || compressed_length != 0) {
1084     ALOGW("Zip: size mismatch on inflated file (%lu vs %" PRIu32 ")",
1085         zstream.total_out, uncompressed_length);
1086     result = kInconsistentInformation;
1087     goto z_bail;
1088   }
1089
1090   result = 0;
1091
1092 z_bail:
1093   inflateEnd(&zstream);    /* free up any allocated structures */
1094
1095   return result;
1096 }
1097
1098 int32_t ExtractToMemory(ZipArchiveHandle handle,
1099                         ZipEntry* entry, uint8_t* begin, uint32_t size) {
1100   ZipArchive* archive = (ZipArchive*) handle;
1101   const uint16_t method = entry->method;
1102   off64_t data_offset = entry->offset;
1103
1104   if (lseek64(archive->fd, data_offset, SEEK_SET) != data_offset) {
1105     ALOGW("Zip: lseek to data at %" PRId64 " failed", (int64_t)data_offset);
```

```
1106    return kIoError;
1107  }


#03 02f398 /system/lib64/libandroidfw.so (ExtractEntryToFile+268)
  ExtractEntryToFile
  system/core/include/utils/FileMap.h:91

 87    /*
 88     * Call this when mapping is no longer needed.
 89     */
 90    void release(void) {
 91        if (--mRefCount <= 0)
 92            delete this;
 93    }


#04 0285a8 /system/lib64/libandroidfw.so (android::ZipFileRO::uncompressEntry(void*, int) const+12)
  android::ZipFileRO::uncompressEntry(void*, int) const
  frameworks/base/libs/androidfw/ZipFileRO.cpp:257
#05 08f27c /system/lib64/libandroid_runtime.so
  android::copyFileIfChanged(_JNIEnv*, void*, android::ZipFileRO*, void*, char const*)
  frameworks/base/core/jni/com_android_internal_content_NativeLibraryHelper.cpp:248

246     // Set the modification time for this file to the ZIP's mod time.
247     struct timeval times[2];
248     times[0].tv_sec = st.st_atime;
249     times[1].tv_sec = modTime;
250     times[0].tv_usec = times[1].tv_usec = 0;
251     if (utimes(localTmpFileName, times) < 0) {
252         ALOGI("Couldn't change modification time on %s: %s\n", localTmpFileName, strerror(errno));
253         unlink(localTmpFileName);
254         return INSTALL_FAILED_CONTAINER_ERROR;
255     }


#06 08f66c /system/lib64/libandroid_runtime.so
  android::iterateOverNativeFiles(_JNIEnv*, long, _jstring*, android::install_status_t (*)(_JNIEnv*, void*, android::ZipFileRO*, void*,
char const*), void*)
  libnativehelper/include/nativehelper/jni.h:851

 850     void ReleaseStringUTFChars(jstring string, const char* utf)
 851     { functions->ReleaseStringUTFChars(this, string, utf); }
 852


#07 08f77c /system/lib64/libandroid_runtime.so
  android::register_com_android_internal_content_NativeLibraryHelper(_JNIEnv*)
  frameworks/base/core/jni/com_android_internal_content_NativeLibraryHelper.cpp:576

573 int register_com_android_internal_content_NativeLibraryHelper(JNIEnv *env)
574 {
575     return AndroidRuntime::registerNativeMethods(env,
576                 "com/android/internal/content/NativeLibraryHelper", gMethods, NELEM(gMethods));
577 }
```

rn...@google.com <rn...@google.com> #3 Oct 29, 2015 11:24PM

Assigned to rn...@google.com.

Hi,
Can you provide the below requested information to better understand the issue:

SDK version
Which version of the SDK are you using?

Android build
Which Android build are you using? (e.g. KVT49L)

Device used
Which device did you use to reproduce this issue?

Steps to reproduce
What steps do others need to take in order to reproduce the issue themselves?

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

Expected output
What do you expect to occur?

Current output
What do you see instead?

logcat output
See http://developer.android.com/tools/help/logcat.html. Copy and paste relevant sections of the logcat output into this issue.

Android bug report
After reproducing the issue, press the volume up, volume down, and power buttons simultaneously. This will capture a bug report on your device in the “bug reports” directory. Attach this file to this issue.

Note: Please upload the bug report and screenshot to google drive and share the folder to android-bugreport@google.com and mention the shared link here.

ji...@gmail.com <ji...@gmail.com> #4 Oct 30, 2015 12:54PM

Hi,
SDK version
None.

Android build
5.0

Device used
Xperia

Steps to reproduce
The 2 fail cases have some different step.
Both them transfer failed/interrupted.
[Condition1]
1.Move media/APP files from internal storage to SD card.
2.Press HW reset pin when DUT was moving files from internal storage to SD card. (DUT will be power off)
3.Power on DUT.

[Condition2]
1.Move media/APP files from internal storage to SD card.
2.Wait transfer finished, but it had been interrupted by un-known reason.
(We implemented a hint window pop-up about this transfer fail scenario.)
3.Reboot DUT

Frequency
Just two times, about 2/50.

Expected output
DUT can boot-up/entering Android OS normally.

Current output
All black screen. No entering android OS and it can't be recovery by reboot.

logcat output
Please refer to attachment

Android bug report
None, please refer to logcat output

deleted
0 B Restricted

en...@google.com <en...@google.com> #5 Oct 31, 2015 02:17AM

do you have the corrupt compressed file in question?

na...@google.com <na...@google.com> #6 Oct 31, 2015 02:23AM

I don't really know whether this is due to a corrupt file, looks more like a race condition to me (i.e, the FileMap was destroyed on another thread)

ji...@gmail.com <ji...@gmail.com> #7 Nov 2, 2015 12:33PM

[Comment deleted]

ji...@gmail.com <ji...@gmail.com> #8 Nov 2, 2015 05:39PM

Hi ,
I don't have the corrupt compressed file.
Actually, I don't know what file is the corrupt file.

na...@google.com <na...@google.com> #9 Nov 5, 2015 09:52PM

+ johan : does this ring a bell over at Sony ? I'm finding it hard to judge whether this is a rare race condition we've never seen or something specific to the device under test.

jo...@sonymobile.com <jo...@sonymobile.com> #10 Nov 6, 2015 02:12AM

We have seen this, yes. The fix for our problem was uploaded here: https://android-review.googlesource.com/#/c/146996/.

na...@google.com <na...@google.com> #11 Nov 6, 2015 02:17AM

Marked as fixed, reassigned to na...@google.com.

Ah right, I'm not sure how I forgot about that change. Excellent memory.

Marking this as Released because this change is in android 6.0. JingCian, feel free to cherry-pick this change into your branches.

Sony folks : thanks (again) for your contribution.