Obsolete Bug P3 +

STATUS UPDATE No update yet. Edit

DESCRIPTION sh...@codeaurora.org created issue #1 May 30, 2017 04:06PM

On setting wrap.<packagename> to ANY value, zygote keeps on crashing.
The error that stands out is this:
E Zygote : Unsupported st_mode 4480
E Zygote : Unsupported st_mode 4480

And the abort message is:
Abort message: 'art/runtime/jni_internal.cc:492] JNI FatalError called: frameworks/base/core/jni/com_android_internal_os_Zygote.cpp:484: Unable to restat file descriptor table.'

Something to do with this pipe-fd being opened
https://android.googlesource.com/platform/frameworks/base/+/master/core/java/com/android/internal/os/ZygoteConnection.java#200

Apitrace has also reported the same issue as on Android, it depends on LD_PRELOAD'ing the trace library using "wrap." property.
https://github.com/apitrace/apitrace/issues/502

Thanks,
Shibin George
Employee of Qualcomm Innovation Center, Inc.
Qualcomm Innovation Center, Inc. is a member of Code Aurora Forum, hosted by The Linux Foundation

Links (8) Hide all

"https://android.googlesource.com/platform/frameworks/base/+/master/core/java/com/android/internal/o... "	sh...@ #1
"https://github.com/apitrace/apitrace/issues/502 "	sh...@ #1
"https://gameguardian.net/forum/topic/18482-android-reboots-after-use-... "	en...@ #3
"https://android.googlesource.com/platform/frameworks/base.git/+/master/core/jni/com_androi... "	en...@ #3
"https://android.googlesource.com/platform/frameworks/base/+/master/c..."	en...@ #3

See all related links

COMMENTS All comments Oldest first

ab...@gmail.com <ab...@gmail.com> #2 Dec 12, 2017 01:14PM

Why it won't work for me

en...@gmail.com <en...@gmail.com> #3 Dec 12, 2017 05:19PM

I described problem here:
https://gameguardian.net/forum/topic/18482-android-reboots-after-use-prevent-protection/
As I see problem in next chain calls before fork() in zygote:

https://android.googlesource.com/platform/frameworks/base.git/+/master/core/jni/com_android_internal_os_Zygote.cpp

static pid_t ForkAndSpecializeCommon(JNIEnv* env, uid_t uid, gid_t gid, jintArray javaGids,

} else if (!gOpenFdTable->Restat(fds_to_ignore)) {

https://android.googlesource.com/platform/frameworks/base/+/master/core/jni/fd_utils.cpp

bool FileDescriptorTable::Restat(const std::vector<int>& fds_to_ignore) {

return RestatInternal(open_fds);

bool FileDescriptorTable::RestatInternal(std::set<int>& open_fds) {

it->second = FileDescriptorInfo::CreateFromFd(*element);

FileDescriptorInfo* FileDescriptorInfo::CreateFromFd(int fd) {

// We only handle whitelisted regular files and character devices. Whitelisted
// character devices must provide a guarantee of sensible behaviour when
// reopened.
//
// S_ISDIR : Not supported. (We could if we wanted to, but it's unused).

Reporter	sh...@codeaurora.o
Type	Bug
Priority	P3
Severity	S3
Status	Won't fix (Obsolete)
Access	Default access View
Assignee	--
Verifier	--
Collaborators	
CC	sh...@codeaurora.org
AOSP ID	--
ReportedBy	--
Found In	--
Targeted To	--
Verified In	--
In Prod	

```
// S_ISLINK : Not supported.
// S_ISBLK : Not supported.
// S_ISFIFO : Not supported. Note that the zygote uses pipes to communicate
// with the child process across forks but those should have been closed
// before we got to this point.
if (!S_ISCHR(f_stat.st_mode) && !S_ISREG(f_stat.st_mode)) {            // <------ f_stat.st_mode == 4480 here
  LOG(ERROR) << "Unsupported st_mode " << f_stat.st_mode;
  return NULL;                                                        // <------ return null
}
```

st_mode 4480 is 00010600, so is S_IFIFO | S_IRUSR | S_IWUSR, so is FIFO (pipe maybe) and cause abort.

This code run before fork(), so it run in zygote process.

It is mean crash zygote. If zygote crashed - phone immediately reboot.

---

mo...@gmail.com <mo...@gmail.com> #4 Mar 25, 2018 03:46PM

this should be fixed by https://android.googlesource.com/platform/frameworks/base/+/8dfa178efbbb155657639bd526e9a8579fce3886

---

ha...@gmail.com <ha...@gmail.com> #5 May 16, 2018 02:36AM

Hello,

Thanks for the fix of broken Wrap functionality at:
https://android.googlesource.com/platform/frameworks/base/+/8dfa178efbbb155657639bd526e9a8579fce3886

Currently, I am using Rooted and SELinux permissive Pixel 2 device for my testing. the pixel2 binary does support the above fix. I am trying to run apitrace and I do get below crash. As crash_dump utility crashes, I don't get any additional crash log and also the tombstone dump.

SELINUX=Permissive
==========

```
05-15 10:42:59.190  1130  1252 I InputReader: Reconfiguring input devices.  changes=0x00000004
05-15 10:42:59.190  1130  1252 I InputReader: Device reconfigured: id=5, name='synaptics_dsxv26', size 1080x1920, orientation 1, mode 1,
display id 0
05-15 10:42:59.191   738   738 I zygote  : Ignoring open file descriptor 3
05-15 10:42:59.192   738   738 I zygote  : Ignoring open file descriptor 4
05-15 10:42:59.215  8771  8771 I app_process32: type=1400 audit(0.0:49): avc: denied { open } for path="/data/libc++_shared.so"
dev="sda45" ino=16 scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:object_r:system_data_file:s0 tclass=file permissive=1
05-15 10:42:59.225  8771  8771 I app_process32: type=1400 audit(0.0:50): avc: denied { execute } for path="/data/libc++_shared.so"
dev="sda45" ino=16 scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:object_r:system_data_file:s0 tclass=file permissive=1
05-15 10:42:59.373   783   803 I CHRE    : @ 328610.062: [AR_CHRE] still: 100
--------- beginning of crash
05-15 10:42:59.469  8771  8771 F libc    : Fatal signal 11 (SIGSEGV), code 1, fault addr 0xff2a6fe8 in tid 8771 (app_process32), pid 8771
(app_process32)
05-15 10:42:59.468  8773  8773 I crash_dump32: type=1400 audit(0.0:51): avc: denied { read } for name="libc++_shared.so" dev="sda45"
ino=16 scontext=u:r:crash_dump:s0:c512,c768 tcontext=u:object_r:system_data_file:s0 tclass=file permissive=1
05-15 10:42:59.505  8771  8771 F libc    : crash_dump helper failed to exec
05-15 10:42:59.505  8771  8771 F libc    : crash_dump helper crashed or stopped
05-15 10:42:59.508   738   738 I Zygote  : Process 8760 exited cleanly (139)
05-15 10:42:59.509   738   738 W Zygote  : Error reading pid from wrapped process, child may have died
05-15 10:42:59.509  1130  6237 I ActivityManager: Start proc 8760:com.rovio.angrybirds/u0a126 for activity
com.rovio.angrybirds/com.rovio.fusion.App
```

If I change SELINUX to enforce, I do get below error.
==========

```
--------- beginning of crash
05-15 11:29:48.249  9502  9502 F libc    : CANNOT LINK EXECUTABLE "/system/bin/app_process32": library "/data/libc++_shared.so" not
found
05-15 11:29:48.249  9502  9502 F libc    : Fatal signal 6 (SIGABRT), code -6 in tid 9502 (app_process32), pid 9502 (app_process32)
05-15 11:29:48.245  9502  9502 W app_process32: type=1400 audit(0.0:56): avc: denied { open } for path="/data/libc++_shared.so"
dev="sda45" ino=16 scontext=u:r:untrusted_app:s0:c512,c768 tcontext=u:object_r:system_data_file:s0 tclass=file permissive=0
05-15 11:29:48.257  9505  9505 I crash_dump32: obtaining output fd from tombstoned, type: kDebuggerdTombstone
05-15 11:29:48.257   868   868 I /system/bin/tombstoned: received crash request for pid 9502
05-15 11:29:48.258  9505  9505 I crash_dump32: performing dump of process 9502 (target tid = 9502)
05-15 11:29:48.258  9505  9505 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
05-15 11:29:48.258  9505  9505 F DEBUG   : Build fingerprint: 'google/walleye/walleye:8.1.0/OPM2.171019.029/4657601:user/release-keys'
05-15 11:29:48.258  9505  9505 F DEBUG   : Revision: 'MP1'
05-15 11:29:48.258  9505  9505 F DEBUG   : ABI: 'arm'
05-15 11:29:48.258  9505  9505 F DEBUG   : pid: 9502, tid: 9502, name: app_process32  >>> /system/bin/app_process32 <<<
05-15 11:29:48.258  9505  9505 F DEBUG   : signal 6 (SIGABRT), code -6 (SI_TKILL), fault addr --------
05-15 11:29:48.259  9505  9505 F DEBUG   : Abort message: 'CANNOT LINK EXECUTABLE "/system/bin/app_process32": library
"/data/libc++_shared.so" not found'
05-15 11:29:48.259  9505  9505 F DEBUG   :    r0 00000000  r1 0000251e  r2 00000006  r3 00000008
05-15 11:29:48.259  9505  9505 F DEBUG   :    r4 0000251e  r5 0000251e  r6 ffe4583c  r7 0000010c
05-15 11:29:48.259  9505  9505 F DEBUG   :    r8 00000000  r9 ffe46adc  sl ffe46ad4  fp f1a4a010
05-15 11:29:48.259  9505  9505 F DEBUG   :    ip ffe45860  sp ffe45828  lr f1ab7f21  pc f1ab6420  cpsr 20070030
05-15 11:29:48.259  9505  9505 F DEBUG   :
05-15 11:29:48.259  9505  9505 F DEBUG   : backtrace:
05-15 11:29:48.259  9505  9505 F DEBUG   :    #00 pc 0005f420  /system/bin/linker (__dl_abort+63)
05-15 11:29:48.259  9505  9505 F DEBUG   :    #01 pc 000101af  /system/bin/linker (__dl___linker_init+2798)
05-15 11:29:48.259  9505  9505 F DEBUG   :    #02 pc 00014f1c  /system/bin/linker (_start+4)
05-15 11:29:48.262  1130  1344 W NativeCrashListener: Couldn't find ProcessRecord for pid 9502
05-15 11:29:48.262   868   868 W /system/bin/tombstoned: crash socket received short read of length 0 (expected 12)
```

05-15 11:29:48.263 1130 1150 I BootReceiver: Copying /data/tombstones/tombstone_04 to DropBox (SYSTEM_TOMBSTONE)
05-15 11:29:48.263 738 738 I Zygote : Process 9491 exited cleanly (134)
05-15 11:29:48.263 738 738 W Zygote : Error reading pid from wrapped process, child may have died
05-15 11:29:48.263 1130 1140 I ActivityManager: Start proc 9491:com.rovio.angrybirds/u0a126 for activity com.rovio.angrybirds/com.rovio.fusion.App

Please see if this is an artifact of code change or something else. This works correctly with Android. 4.x version without any issue.

Thanks,
Hardik

gy...@gmail.com <gy...@gmail.com> #6 Mar 31, 2020 04:02AM

《TS》KORONA

sa...@google.com <sa...@google.com> #7 Aug 19, 2020 01:19AM

Status: Won't Fix (Obsolete)

Thank you for your feedback. We assure you that we are doing our best to address all issues reported. For now, we will be closing the issue as won't fix obsolete. If this issue currently still exists, we request that you log a new issue along with the bug report here https://goo.gl/TbMiIO and reference this bug for context.