Android Public Tracker 175959407

when i use HIDL Java transact native handle ,i get an error about SELinux

+1 Hotlists (7) Mark as Duplicate

Comments (12) Dependencies Duplicates (0) Blocking (0) Resources (4)

WAI Bug P3 + [AOSP] assigned

STATUS UPDATE No update yet. Edit

Reporter	ma...@gmail.com
Type	Bug
Priority	P3
Severity	S3
Status	Won't fix (Intended behavior)
Access	Default access View
Assignee	am...@google.com
Verifier	--
Collaborators	
CC	am...@google.com ma...@gmail.com
AOSP ID	--
ReportedBy	Developer
Found In	--
Targeted To	--
Verified In	--
In Prod	

DESCRIPTION ma...@gmail.com created issue #1 Dec 19, 2020 01:52PM

i use follow code to debug HIDL java:

```
IRichtapVibrator.performRtpCallback callback = new IRichtapVibrator.performRtpCallback(){
              @Override public void onValues(int retStatus, int retLengthMs) {
                  int status = retStatus;
                  long lengthMs = (long)retLengthMs;
                  Slog.d(TAG, "aac richtap performRtpCallback, status:"+status+",lengthMs:"+lengthMs);
              }
          };
NativeHandle handle = new NativeHandle(pfd.getFileDescriptor(),false);
service.performRtp(handle, callback);
```

i get an error:

```
12-18 05:53:46.350 I/auditd  ( 1550): type=1400 audit(0.0:13): avc: denied { use } for comm="Binder:1550_E" path="/dev/ashmemfe8fcfc6-32b7-408c-8aaf-09aeb2318eed" dev="tmpfs" ino=1778 scontext=u:r:hal_vibrator_default:s0 tcontext=u:r:untrusted_app_27:s0:c512,c768 tclass=fd permissive=0
12-18 05:53:46.350 W/Binder:1550_E( 1550): type=1400 audit(0.0:13): avc: denied { use } for path="/dev/ashmemfe8fcfc6-32b7-408c-8aaf-09aeb2318eed" dev="tmpfs" ino=1778 scontext=u:r:hal_vibrator_default:s0 tcontext=u:r:untrusted_app_27:s0:c512,c768 tclass=fd permissive=0
```

i wanna know how can i resolve this SELinux. i don't think add sepolicy is a good way. on my mind , native handle should resolve this SELinux. i can't be sure if it is a bug. please help me . thanks

✓ Links (4) Hide all

"For steps to capture a bug report, please refer: https://developer.android.com/studio/debug/bug-report#bugreportdevice"	am...@ #2
"http://ro.build.id"	ma...@ #3
"https://drive.google.com/file/d/1NtVqQSo_MtoQpVEU2hAhWHnQZO8qMco… "	ma...@ #3
"https://drive.google.com/file/d/14FnRw061UPmhIQFumw-9OGnUbo4N41C… "	ma...@ #3

COMMENTS All comments ↓ Oldest first

am...@google.com <am...@google.com> Dec 21, 2020 02:12PM

Assigned to am...@google.com.

am...@google.com <am...@google.com> #2 Dec 21, 2020 06:19PM

Thank you for reporting this issue. For us to further investigate this issue, please provide the following additional information:

What SDK version are you using?

Which Android build are you using? (e.g. PPP5.180610.010)

Which device did you use to reproduce this issue?

Please provide sample project or apk to reproduce the issue. Also mention the steps to be followed for reproducing the issue with the given sample project or apk.

Android bug report (to be captured after reproducing the issue)
For steps to capture a bug report, please refer: https://developer.android.com/studio/debug/bug-report#bugreportdevice

Alternate method
Navigate to "Developer options", ensure "USB debugging" is enabled, then enable "Bug report shortcut". Capture bug report by holding the power button and selecting the "Take bug report" option.

Note: Please upload the bug report and app to google drive and share the folder to android-bugreport@google.com, then share the link here.

ma...@gmail.com <ma...@gmail.com> #3 Dec 22, 2020 01:11PM

thanks for your reply
What SDK version are you using?
--->30, i use aosp android-11.0.0_r17 to build the image

Which Android build are you using?
--->ro.build.id=RP1A.201105.002 / ro.build.version.security_patch=2020-11-05 / ro.build.description=aosp_coral-userdebug 11 RP1A.201105.002 eng.xxxxx.20201217.114700 test-keys
Which device did you use to reproduce this issue?
----> i use pixel 4 for developing this function. and i add a hal interface. in framewok ,i write performRtp function to call hal.

sample code:
on app(sdk 27):
create a MemoryFile , and transact ParcelFileDescriptor to framework/service
on framework/service:
get the ParcelFileDescriptor， and create a NativeHandle, then transact NativeHandle to hidl

now
i got this error:

```
12-14 11:46:08.320 W/Binder:1495_4( 1495): type=1400 audit(0.0:29): avc: denied { use } for path="/dev/ashmem9f6c1bdf-0fb1-454e-8489-c1a1000c64ea" dev="tmpfs" ino=16470 scontext=u:r:hal_vibrator_default:s0 tcontext=u:r:untrusted_app_27:s0:c512,c768 tclass=fd permissive=0
```

for my mind:
NativeHandle should solve this SELinux issue。expect your reply.

sample code:
https://drive.google.com/file/d/1NtVqQSo_MtoQpVEU2hAhWHnQZO8qMco_/view?usp=sharing
log link:
https://drive.google.com/file/d/14FnRw061UPmhIQFumw-9OGnUbo4N41CJ/view?usp=sharing

am...@google.com <am...@google.com> #4 Dec 22, 2020 06:37PM

Thank you for reporting this issue. We’ve shared this with our product and engineering teams and will continue to provide updates as more information becomes available.

am...@google.com <am...@google.com> #5 Dec 24, 2020 05:23PM

IRichtapVibrator.performRtpCallback performRtp

This looks like a custom HAL extension. Since this new interface requires passing a native handle, and the permissions for that aren't currently allowed, either:

the interface should be changed to avoid needing a native handle
the permission should be added to use the native handle
Without a detailed analysis of the design/etc.. of this interface, it's impossible to say what is right from a security perspective or what is required technically.

I use follow code to debug HIDL java

If this is for testing only, you may consider the sepolicy macro userdebug_or_eng which can be used to avoid giving this permission in production.

ma...@gmail.com <ma...@gmail.com> #6 Dec 24, 2020 06:07PM

Dear
thanks for your reply.
i can add sepolicy change for resolving this SELinux issue. i want to known if it is normal.
on Android Q ,i use c++ backend to transact handle. it's ok .do not have SELinux issue.
sample code:

```
      hidl_handle hanle;
      native_handle_t *nh = native_handle_create(1,0);
      nh->data[0] = fd;
      hanle.setTo(nh, false /*own*/);
      //ALOGD("hidl handle ,set to not own this fd.");

      halCall(&RICHTAP::IVibrator::performRtp, static_cast<hidl_handle>(hanle), callback);
```

on Android 11, use same code(c++ backend), from jni to hal, also have SELinux issue. of course, java backend still has this SELinux issue.
could you help me to check why Android 11 show me this issue , Android Q not.
Android 11 upgrade security level?
expect your reply, thanks in advance for your help.

am...@google.com <am...@google.com> #7 Dec 28, 2020 06:52PM

Thanks for your update. We'll let you know soon.

am...@google.com <am...@google.com> #8 Dec 29, 2020 06:02PM

Hi mash...@,

Below is the response for your comment#6.

============
Transfer of a file descriptor should be blocked by SELinux. It sounds like either:

There was a bug that was fixed

OR

The permission was removed so that you had to add it randomly
Otherwise, if the issue still exists now, since you need the permission now, it seems we have no way of reproducing it. If you can reproduce it still, 1/2 should be ruled out.

ma...@gmail.com <ma...@gmail.com> #9 Dec 31, 2020 11:53AM

Dear am...@google.com
thanks for your reply, but how i can confirm SeLinux issue was fixed or should i add permission?
my version tag is refs/tags/android-11.0.0_r17
if i add this permission for transferring file descriptor, if it cause XTS fail or not ?

am...@google.com <am...@google.com> #10 Jan 6, 2021 05:49PM

Hi mash...@,

If there is a denial, then a permission is needed for this to work.

if I add this permission for transferring file descriptor, if it cause XTS fail or not ?

CTS tests neverallow rules, which are also evaluated at compile time. So, if this builds (without removing neverallow rules), then it should pass this test case. I don't suspect any other test would fail, but you would need to run it to be sure.

Let us know for any other concerns.

ma...@gmail.com <ma...@gmail.com> #11 Jan 12, 2021 12:36PM

thanks for your reply . it's clear for me, and this tracker can be closed . thanks again.

am...@google.com <am...@google.com> #12 Jan 12, 2021 08:03PM

Status: Won't Fix (Intended Behavior)

Thanks for the update. Closing it as per comment#11.