Android Public Tracker 205880718

bootchart not working on android 12

+1 4 Hotlists (4) Mark as Duplicate

Comments (3) Dependencies Duplicates (0) Blocking (0) Resources (1)

Fixed Bug P3 + Add Hotlist [AOSP] assigned

STATUS UPDATE No update yet. Edit

DESCRIPTION ji...@nxp.com created issue #1 Nov 11, 2021 07:49PM

Hi Google Friends,

We found that the bootchart is not working on android 12, one selinux denied was observed:

```
   [    8.769133] type=1400 audit(1636343280.852:3): avc: denied { mounton } for comm="apexd"
path="/apex/apex-info-list.xml" dev="tmpfs" ino=13 scontext=u:r:apexd:
s0 tcontext=u:object_r:apex_info_file:s0 tclass=file permissive=1
```

It will cause the runtime abort like below:

```
11-08 02:56:49.694  5735  5735 I crash_dump64: performing dump of process 5683 (target tid = 5683)
11-08 02:56:49.709  5735  5735 E DEBUG   : failed to read /proc/uptime: Permission denied
11-08 02:56:49.781  5687  5687 F nativeloader: Error finding namespace of apex: no namespace called
com_android_art
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669] Runtime aborting...
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669] Dumping all threads without mutator lock held
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669] All threads:
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669] DALVIK THREADS (1):
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669] "main" prio=10 tid=1 Runnable (still starting up)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   | group="" sCount=0 ucsCount=0 flags=0 obj=0x0
self=0xd9f83810
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   | sysTid=5687 nice=-20 cgrp=top-app sched=0/0
handle=0xe8738470
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   | state=R schedstat=( 602423375 180169250 53 )
utm=43 stm=16 core=3 HZ=100
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   | stack=0xff416000-0xff418000 stackSize=8188KB
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   | held mutexes= "abort lock" "mutator lock"(shared
held)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #00 pc 00375641
 /apex/com.android.art/lib/libart.so (art::DumpNativeStack(std::__1::basic_o
stream<char, std::__1::char_traits<char> >
&, int, BacktraceMap*, char const*, art::ArtMethod*, void*, bool)+76)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #01 pc 0044dc27
 /apex/com.android.art/lib/libart.so (art::Thread::DumpStack(std::__1::basic
_ostream<char, std::__1::char_traits<char>
 >&, bool, BacktraceMap*, bool) const+214)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #02 pc 00465701
 /apex/com.android.art/lib/libart.so (art::DumpCheckpoint::Run(art::Thread*)
+656)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #03 pc 00460c5d
 /apex/com.android.art/lib/libart.so (art::ThreadList::RunCheckpoint(art::Cl
osure*, art::Closure*)+348)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #04 pc 0046019f
 /apex/com.android.art/lib/libart.so (art::ThreadList::Dump(std::__1::basic_
ostream<char, std::__1::char_traits<char>
>&, bool)+1222)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #05 pc 0040c82b
 /apex/com.android.art/lib/libart.so (art::Runtime::Abort(char const*)+1770)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #06 pc 0000f59d
 /apex/com.android.art/lib/libbase.so (android::base::SetAborter(std::__1::f
unction<void (char const*)>&&)::$_3::__inv
oke(char const*)+48)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #07 pc 00004fab  /system/lib/liblog.so
(__android_log_assert+158)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #08 pc 00009517
 /apex/com.android.art/lib/libnativeloader.so (OpenNativeLibrary+1710)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #09 pc 002a134f
 /apex/com.android.art/lib/libart.so (art::JavaVMExt::LoadNativeLibrary(_JNI
Env*, std::__1::basic_string<char, std::__
1::char_traits<char>, std::__1::allocator<char> > const&, _jobject*, _jclass*, std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char
```

Reporter	ji...@nxp.com
Type	Bug
Priority	P3
Severity	S3
Status	Fixed
Access	Default access View
Assignee	am...@google.com
Verifier	--
Collaborators	
CC	am...@google.com ji...@nxp.com
AOSP ID	--
ReportedBy	Developer
Found In	--
Targeted To	--
Verified In	--
In Prod	

```
> >*)+1698)
11-08 02:56:49.882  5687  5687 F zygote  : runtime.cc:669]   native: #10 pc 00414fb7
 /apex/com.android.art/lib/libart.so (art::Runtime::InitNativeMethods()+158)

11-08 02:56:49.889   240   240 I logd    : logdr: UID=0 GID=0 PID=5735 n tail=0 logMask=8 pid=5683 start=0ns
deadline=0ns
11-08 02:56:49.904   240   240 I logd    : logdr: UID=0 GID=0 PID=5735 n tail=0 logMask=1 pid=5683 start=0ns
deadline=0ns
11-08 02:56:49.925  5735  5735 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
11-08 02:56:49.925  5735  5735 F DEBUG   : Build fingerprint:
'Android/evk_8mm/evk_8mm:12/SP1A.211105.002.A1/eng.nxf362.20211108.104533:userdebug/dev-keys'
11-08 02:56:49.925  5735  5735 F DEBUG   : Revision: '0'
11-08 02:56:49.925  5735  5735 F DEBUG   : ABI: 'arm64'
11-08 02:56:49.925  5735  5735 F DEBUG   : Timestamp: 2021-11-08 02:56:49.709306250+0000
11-08 02:56:49.925  5735  5735 F DEBUG   : Process uptime: 0s
11-08 02:56:49.925  5735  5735 F DEBUG   : Cmdline: zygote64
11-08 02:56:49.925  5735  5735 F DEBUG   : pid: 5683, tid: 5683, name: main  >>> zygote64 <<<
11-08 02:56:49.925  5735  5735 F DEBUG   : uid: 0
11-08 02:56:49.925  5735  5735 F DEBUG   : tagged_addr_ctrl: 0000000000000001
11-08 02:56:49.925  5735  5735 F DEBUG   : signal 6 (SIGABRT), code -1 (SI_QUEUE), fault addr --------
11-08 02:56:49.925  5735  5735 F DEBUG   : Abort message: 'Error finding namespace of apex: no namespace
called com_android_art'
11-08 02:56:49.925  5735  5735 F DEBUG   :     x0  0000000000000000  x1  0000000000001633  x2
 0000000000000006  x3  0000007fda2e0020
11-08 02:56:49.925  5735  5735 F DEBUG   :     x4  0000000000000a6e  x5  0000000000000a6e  x6
 0000000000000a6e  x7  0000000000000a6e
11-08 02:56:49.925  5735  5735 F DEBUG   :     x8  00000000000000f0  x9  000000763e8dd0b0  x10
ffffff00fffffbdf  x11 0000000000000001
11-08 02:56:49.925  5735  5735 F DEBUG   :     x12 0000fffffffff3ff  x13 000000007fffffff  x14
0000000000036bd0  x15 00000000ea3df741
11-08 02:56:49.925  5735  5735 F DEBUG   :     x16 000000763e97d050  x17 000000763e959700  x18
00000076576d4000  x19 00000000000000ac
11-08 02:56:49.925  5735  5735 F DEBUG   :     x20 0000000000001633  x21 00000000000000b2  x22
0000000000001633  x23 00000000ffffffff
11-08 02:56:49.925  5735  5735 F DEBUG   :     x24 00000074132b618e  x25 0000000000000002  x26
b4000074348a3c90  x27 000000741329378c
11-08 02:56:49.926  5735  5735 F DEBUG   :     x28 0000007413c17000  x29 0000007fda2e00a0
11-08 02:56:49.926  5735  5735 F DEBUG   :     lr  000000763e90aefc  sp  0000007fda2e0000  pc
 000000763e90af2c  pst 0000000000000000
11-08 02:56:49.926  5735  5735 F DEBUG   : backtrace:
11-08 02:56:49.926  5735  5735 F DEBUG   :       #00 pc 000000000004ff2c
 /apex/com.android.runtime/lib64/bionic/libc.so (abort+180) (BuildId: ac3d0baaacdc7c6cde
bcc4f2fe5705dd)
11-08 02:56:49.926  5735  5735 F DEBUG   :       #01 pc 000000000062f1ec
 /apex/com.android.art/lib64/libart.so (art::Runtime::Abort(char const*)+764) (BuildId:
7bc69c153455222a1c7a69fdf7cc15ef)
11-08 02:56:49.926  5735  5735 F DEBUG   :       #02 pc 0000000000015aa0
 /apex/com.android.art/lib64/libbase.so (android::base::SetAborter(std::__1::function<vo
id (char const*)>&&)::$_3::__invoke(char c
onst*)+80) (BuildId: fc58b011b253e095bf1244e588fb3b2a)
11-08 02:56:49.926  5735  5735 F DEBUG   :       #03 pc 0000000000006e3c  /system/lib64/liblog.so
(__android_log_assert+308) (BuildId: 8c9b234f4a12a6d67d7ff8f4e7
7c0659)
11-08 02:56:49.926  5735  5735 F DEBUG   :       #04 pc 000000000000cde4
 /apex/com.android.art/lib64/libnativeloader.so (OpenNativeLibrary+2292) (BuildId: d7843
67732e5a77414ccb9ad99ca23fa)
11-08 02:56:49.926  5735  5735 F DEBUG   :       #05 pc 0000000000458460
 /apex/com.android.art/lib64/libart.so (art::JavaVMExt::LoadNativeLibrary(_JNIEnv*, std:
:__1::basic_string<char, std::__1::char_tr
aits<char>, std::__1::allocator<char> > const&, _jobject*, _jclass*, std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> >*)+2144
) (BuildId: 7bc69c153455222a1c7a69fdf7cc15
ef)
11-08 02:56:49.926  5735  5735 F DEBUG   :       #06 pc 000000000063afd4
 /apex/com.android.art/lib64/libart.so (art::Runtime::InitNativeMethods()+204) (BuildId:
 7bc69c153455222a1c7a69fdf7cc15ef)
11-08 02:56:49.926  5735  5735 F DEBUG   :       #07 pc 00000000006381ec
 /apex/com.android.art/lib64/libart.so (art::Runtime::Start()+1964) (BuildId: 7bc69c1534
```

One fix has been pushed to: https://android-review.googlesource.com/c/platform/system/sepolicy/+/1888457
Could you please check this? Thanks!

COMMENTS

All comments ▼ ↓ Oldest first

am...@google.com <am...@google.com> Nov 11, 2021 08:41PM

Assigned to am...@google.com.

am...@google.com <am...@google.com> #2 Nov 11, 2021 10:31PM

Thank you for the report. We’ve shared this with our product and engineering teams and will continue to provide updates as more information becomes available.
In the mean while, please do address the queries asked in the patch.

am...@google.com <am...@google.com> #3 Nov 17, 2021 07:57PM

Marked as fixed.

The change was merged. Hence closing it.