AudioPolicyService server died! ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 in system_server

Infeasible Bug P3 + Add Hotlist

STATUS UPDATE No update yet. Edit

DESCRIPTION hu...@gmail.com created issue #1 Apr 22, 2023 11:39PM

While fuzz testing the Android native system service, I found a java exception triggered by a null pointer dereference that would cause the process to crash and generate a tombstone file, The detail of tombstone is below:

*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
'Android/aosp_taimen/taimen:9/PQ3A.190801.002/root02252256:userdebug/test-keys'
'rev_10'
'arm64'
32431, tid: 32617, name: Binder:32431_4 >>> system_server <<<
signal 6 (SIGABRT), code -6 (SI_TKILL), fault addr --------
claimed length = 3462
x0 0000000000000000 x1 0000000000007f69 x2 0000000000000006 x3 0000000000000008
x4 4d4853514e41403c x5 4d4853514e41403c x6 4d4853514e41403c x7 7f7f7f7f7f7f7f7f
x8 0000000000000083 x9 0000007af81389a0 x10 ffffffff87ffffbdf x11 0000000000000001
x12 0000000000000007 x13 0000000000000000 x14 0000000000000006 x15 0000000000000000
x16 0000007af81712c8 x17 0000007af80af2d8 x18 0000000000000004 x19 0000000000007eaf
x20 0000000000007f69 x21 0000000000000083 x22 0000007af19473b8 x23 0000007af23510f0
x24 0000000000000040 x25 0000007ac872f588 x26 000000618c7b26c0 x27 000000000000000b
x28 000000618c7b1008 x29 0000007ac83f9130
sp 0000007ac83f90f0 lr 0000007af80a3a90 pc 0000007af80a3abc

backtrace:
#00 pc 0000000000021abc /system/lib64/libc.so (abort+124)
#01 pc 0000000000033690 /system/lib64/libclang_rt.asan-aarch64-android.so (__sanitizer::Abort()+56)
#02 pc 0000000000031250 /system/lib64/libclang_rt.asan-aarch64-android.so (__sanitizer::Die()+164)
#03 pc 00000000000a1fd0 /system/lib64/libclang_rt.asan-aarch64-android.so (__asan::ScopedInErrorReport::~ScopedInErrorReport()+316)
#04 pc 00000000000a092c /system/lib64/libclang_rt.asan-aarch64-android.so (__asan::ReportDeadlySignal(__sanitizer::SignalContext const&)+156)
#05 pc 00000000000a0360 /system/lib64/libclang_rt.asan-aarch64-android.so (__asan::AsanOnDeadlySignal(int, void*, void*)+80)
#06 pc 0000000000003924 /system/bin/app_process64 (art::SignalChain::Handler(int, siginfo*, void*)+348)
#07 pc 000000000000088c [vdso:0000007af8a06000]
#08 pc 000000000000aa6c /data/asan/system/lib64/libcutils.so (native_handle_close+52)
#09 pc 000000000001123c /data/asan/system/lib64/libsensor.so (android::BnSensorServer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+1716)
#10 pc 0000000000055938 /data/asan/system/lib64/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+200)
#11 pc 00000000000072ad8 /data/asan/system/lib64/libbinder.so (android::IPCThreadState::executeCommand(int)+1312)
#12 pc 0000000000072390 /data/asan/system/lib64/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+320)
#13 pc 00000000000735c4 /data/asan/system/lib64/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+60)
#14 pc 00000000000cf790 /data/asan/system/lib64/libbinder.so (android::PoolThread::threadLoop()+56)
#15 pc 00000000000168a4 /data/asan/system/lib64/libutils.so (android::Thread::_threadLoop(void*)+804)
#16 pc 00000000000c3d94 /data/asan/system/lib64/libandroid_runtime.so (android::AndroidRuntime::javaThreadShell(void*)+500)
#17 pc 0000000000083114 /system/lib64/libc.so (__pthread_start(void*)+36)
#18 pc 00000000000233bc /system/lib64/libc.so (__start_thread+68)
==32431==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x007af368fa70 bp 0x007ac872ea30 sp 0x007ac872ea00 T104)

==32431==The signal is caused by a READ memory access.

==32431==Hint: address points to the zero page.

#21 0x7af368fa6f in native_handle_close system/core/libcutils/native_handle.cpp:84

#22 0x7af53d023f in android::BnSensorServer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int) frameworks/native/libs/sensor/ISensorServer.cpp:204

#23 0x7af3c2393b in android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int) frameworks/native/libs/binder/Binder.cpp:129

#24 0x7af3c40adb in android::IPCThreadState::executeCommand(int) frameworks/native/libs/binder/IPCThreadState.cpp:1121

#25 0x7af3c40393 in android::IPCThreadState::getAndExecuteCommand() frameworks/native/libs/binder/IPCThreadState.cpp:458

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

#26 0x7af3c415c7 in android::IPCThreadState::joinThreadPool(bool) frameworks/native/libs/binder/IPCThreadState.cpp:538

#27 0x7af3c9d793 in android::PoolThread::threadLoop() frameworks/native/libs/binder/ProcessState.cpp:61

#28 0x7af27508a7 in android::Thread::_threadLoop(void*) system/core/libutils/Threads.cpp:744

#29 0x7af4c21d97 in android::AndroidRuntime::javaThreadShell(void*) frameworks/base/core/jni/AndroidRuntime.cpp:1255

#30 0x7af8105117 in __pthread_start(void*) bionic/libc/bionic/pthread_create.cpp:248

#31 0x7af80a53bf in __start_thread bionic/libc/bionic/clone.cpp:52

uid=1000(system) Binder:32431_4 identical 4 lines

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV (/data/asan/system/lib64/libcutils.so+0xaa6f)

Thread T104 (Binder:32431_4) created by T12 (Binder:32431_2) here:

#0 0x7af16549bf (/system/lib64/libclang_rt.asan-aarch64-android.so+0x8a9bf)

#32 0x7af274f867 in androidCreateRawThreadEtc system/core/libutils/Threads.cpp:153

#33 0x7af275036f in androidCreateThreadEtc system/core/libutils/Threads.cpp:289
#34 0x7af275036f in android::createThreadEtc(int (*)(void*), void*, char const*, int, unsigned long, void**) system/core/libutils/include/utils/AndroidThreads.h:111
#35 0x7af275036f in android::Thread::run(char const*, int, unsigned long) system/core/libutils/Threads.cpp:686

#36 0x7af3c9b82f in android::ProcessState::spawnPooledThread(bool) frameworks/native/libs/binder/ProcessState.cpp:358

#37 0x7af3c40813 in android::IPCThreadState::executeCommand(int) frameworks/native/libs/binder/IPCThreadState.cpp:1179

#38 0x7af3c40393 in android::IPCThreadState::getAndExecuteCommand() frameworks/native/libs/binder/IPCThreadState.cpp:458

#39 0x7af3c415c7 in android::IPCThreadState::joinThreadPool(bool) frameworks/native/libs/binder/IPCThreadState.cpp:538

#40 0x7af3c9d793 in android::PoolThread::threadLoop() frameworks/native/libs/binder/ProcessState.cpp:61

#41 0x7af27508a7 in android::Thread::_threadLoop(void*) system/core/libutils/Threads.cpp:744

#42 0x7af4c21d97 in android::AndroidRuntime::javaThreadShell(void*) frameworks/base/core/jni/AndroidRuntime.cpp:1255

#43 0x7af8105117 in __pthread_start(void*) bionic/libc/bionic/pthread_create.cpp:248

#44 0x7af80a53bf in __start_thread bionic/libc/bionic/clone.cpp:52

Thread T12 (Binder:32431_2) created by T11 (Binder:32431_1) here:

#0 0x7af16549bf (/system/lib64/libclang_rt.asan-aarch64-android.so+0x8a9bf)

#45 0x7af274f867 in androidCreateRawThreadEtc system/core/libutils/Threads.cpp:153

#46 0x7af275036f in androidCreateThreadEtc system/core/libutils/Threads.cpp:289
#47 0x7af275036f in android::createThreadEtc(int (*)(void*), void*, char const*, int, unsigned long, void**) system/core/libutils/include/utils/AndroidThreads.h:111
#48 0x7af275036f in android::Thread::run(char const*, int, unsigned long) system/core/libutils/Threads.cpp:686

#49 0x7af3c9b82f in android::ProcessState::spawnPooledThread(bool) frameworks/native/libs/binder/ProcessState.cpp:358

#50 0x7af3c40813 in android::IPCThreadState::executeCommand(int) frameworks/native/libs/binder/IPCThreadState.cpp:1179

#51 0x7af3c40393 in android::IPCThreadState::getAndExecuteCommand() frameworks/native/libs/binder/IPCThreadState.cpp:458

#52 0x7af3c415c7 in android::IPCThreadState::joinThreadPool(bool) frameworks/native/libs/binder/IPCThreadState.cpp:538

#53 0x7af3c9d793 in android::PoolThread::threadLoop() frameworks/native/libs/binder/ProcessState.cpp:61

#54 0x7af27508a7 in android::Thread::_threadLoop(void*) system/core/libutils/Threads.cpp:744

#55 0x7af4c21d97 in android::AndroidRuntime::javaThreadShell(void*) frameworks/base/core/jni/AndroidRuntime.cpp:1255

#56 0x7af8105117 in __pthread_start(void*) bionic/libc/bionic/pthread_create.cpp:248

#57 0x7af80a53bf in __start_thread bionic/libc/bionic/clone.cpp:52

Thread T11 (Binder:32431_1) created by T0 (system_server) here:

#0 0x7af16549bf (/system/lib64/libclang_rt.asan-aarch64-android.so+0x8a9bf)

#58 0x7af274f867 in androidCreateRawThreadEtc system/core/libutils/Threads.cpp:153

#59 0x7af275036f in androidCreateThreadEtc system/core/libutils/Threads.cpp:289
#60 0x7af275036f in android::createThreadEtc(int (*)(void*), void*, char const*, int, unsigned long, void**) system/core/libutils/include/utils/AndroidThreads.h:111
#61 0x7af275036f in android::Thread::run(char const*, int, unsigned long) system/core/libutils/Threads.cpp:686

#62 0x7af3c9b82f in android::ProcessState::spawnPooledThread(bool) frameworks/native/libs/binder/ProcessState.cpp:358

#63 0x7af3c9b5d7 in android::ProcessState::startThreadPool() frameworks/native/libs/binder/ProcessState.cpp:162

#64 0x618c794497 in android::AppRuntime::onZygoteInit() frameworks/base/cmds/app_process/app_main.cpp:95

#65 0x73375bb3 in

==32431==ABORTING

AudioPolicyService server died!
Sound trigger service died!
AudioFlinger server died!
Audioserver died.
hidl_ssvc_poll: spurious wake up, back to work
Audioserver started.
--------- log main
uid=0(root) system_server expire 1 line
setrlimit(RLIMIT_CORE) failed for pid 32431: Operation not permitted
Process: zygote socket RESERVED/zygote_secondary opened, supported ABIS: armeabi-v7a,armeabi
The ClassLoaderContext is a special shared library.
uid=1000 system_server identical 2 lines
The ClassLoaderContext is a special shared library.
Can't register UsbAlsaJackDetector native methods
Bluetooth binder is null
Loaded power HAL 1.0 service
Loaded power HAL 1.1 service

✓ Links (2) Hide all

“http://libclang_rt.asan-aarch64-android.so” hu...@ #1
“ … steps to capture a bug report, please refer: https://developer.android.com/studio/debug/bug-report#bugreportdevice” vi...@ #2

COMMENTS All comments ↓ Oldest first

vi...@google.com <vi...@google.com> #2 Apr 23, 2023 06:38PM

Assigned to vi...@google.com.

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

What steps are needed to reproduce this issue? Frequency of occurrence?

Which Android build are you using? (e.g. OPP1.170223.012)

Which device did you use to reproduce this issue?

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 screenshot to google drive and share the folder to android-bugr

su...@google.com <su...@google.com> #3 Apr 29, 2023 07:15PM

Please provide the requested information to proceed further. Unfortunately the issue will be closed within 7 days if there is no further update.

vi...@google.com <vi...@google.com> #4 May 6, 2023 12:07AM

Status: Won't Fix (Infeasible)

We are closing this issue since we didn't receive a response. If you are still facing this problem, please open a new issue and add the relevant information along with reference to this issue.