

Figure - Bug #118915

【AF】【VC1】【台架】【副屏】语音通话时 打开原神等待启动完成 挂断语音（QQ） 原神界面短暂停留后 闪退

2023-06-28 16:32 - 物联网测试组_TSCD 王维

Status:	ASSIGNED	Start date:	2023-06-28
Priority:	Normal	Due date:	
Assignee:	Multimedia组-RD3_TSCD 梁卿山	% Done:	0%
Category:	AUDIO-FW	Estimated time:	0.00 hour
Target version:		Found Version:	FlatBuild_HH_MCE_FSE.M.D.user.01.00.C106(X106)
Need_Info:	--	Degrated:	--
Resolution:	WONTFIX	Verified Version:	
Severity:	Normal	Fixed Version:	
Reproducibility:	Occasionally	Root cause:	
Test Type:	ST		

Description

【环境信息】
台架

【前提条件】
1.设备正常上电
2.副屏已下对应的应用程序，且待更新（王者荣耀 火影忍者）

【操作步骤】
1.副屏接到QQ语音来电处于通话中
2.打开原神并等待启动完成
3.挂断语音通话

【实际结果】
原神在短暂播放动画后会出现闪退

【期望结果】
原神正常运行不会出现异常现象

History

#1 - 2023-06-28 16:45 - CD FW 曹覃刚

- Category changed from CD-APP to AUDIO-FW

- Assignee changed from CD FW 曹覃刚 to Multimedia组-RD3_TSCD 梁卿山

Hi 卿山

如沟通，报了下面的音频错误导致原生崩了，请帮助分析

06-28 16:23:06.392 2154 2154 F DEBUG : *

06-28 16:23:06.393 2154 2154 F DEBUG : Build fingerprint: 'HiPhi/PassengerDisplay_CN/PassengerDisplay:12/SKQ1.220201.001/4365:user/release-keys'

06-28 16:23:06.393 2154 2154 F DEBUG : Revision: '0'

06-28 16:23:06.393 2154 2154 F DEBUG : ABI: 'arm64'

06-28 16:23:06.393 2154 2154 F DEBUG : Timestamp: 2023-06-28 16:23:03.858813437+0800

06-28 16:23:06.393 2154 2154 F DEBUG : Process uptime: 0s

06-28 16:23:06.393 2154 2154 F DEBUG : Cmdline: com.miHoYo.Yuanshen

06-28 16:23:06.393 2154 2154 F DEBUG : pid: 32394, tid: 1774, name: AudioTrack >>> com.miHoYo.Yuanshen <<<

06-28 16:23:06.393 2154 2154 F DEBUG : uid: 10072

```
06-28 16:23:06.393 2154 2154 F DEBUG : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x0
06-28 16:23:06.393 2154 2154 F DEBUG : Cause: null pointer dereference
06-28 16:23:06.393 2154 2154 F DEBUG : x0 0000000000000000 x1 0000000000000000 x2 0000000000000001 x3 0000000000000000
06-28 16:23:06.393 2154 2154 F DEBUG : x4 0000000000000000 x5 0000000000000480 x6 0000000000000090 x7 ff736d746e426d74
06-28 16:23:06.393 2154 2154 F DEBUG : x8 00000000000000c0 x9 0000006d7bba83cf x10 0000006d7bba83cf x11 0000000000000049
06-28 16:23:06.393 2154 2154 F DEBUG : x12 0000000000000049 x13 0000006d88bf01e8 x14 0000000000000008 x15 0000006c98f4f000
06-28 16:23:06.393 2154 2154 F DEBUG : x16 0000006d7bbdf240 x17 00000070b020c16c x18 0000006c38620000 x19 b400006d6c1a85b0
06-28 16:23:06.393 2154 2154 F DEBUG : x20 0000000000000090 x21 0000000000000000 x22 0000006d88bf1ae8 x23 b400006e5c2ee210
06-28 16:23:06.393 2154 2154 F DEBUG : x24 b400006d6c1a85f8 x25 00000070a3ec0970 x26 0000000000000009 x27 00000070a3e32010
06-28 16:23:06.393 2154 2154 F DEBUG : x28 0000006c98f4e9e8 x29 0000006c98f4e860
06-28 16:23:06.393 2154 2154 F DEBUG : lr 0000006c891a2920 sp 0000006c98f4e860 pc 0000006c8917de34 pst 0000000020001000
06-28 16:23:06.393 2154 2154 F DEBUG : backtrace:
06-28 16:23:06.393 2154 2154 F DEBUG : #00 pc 00000000001dae34
/data/app/~~_ONPenk8dLGLa3bFJVgmjg==/com.miHoYo.Yuanshen-HU10quAflWxuUB6-bLtjxA==/lib/arm64/libMmoron.so
(CAKSink::OnIncompleteWrite(unsigned int)+44) (BuildId: c94f76a9baa34f596e39c45d05e918c4f77834ff)
06-28 16:23:06.393 2154 2154 F DEBUG : #01 pc 00000000001ff91c
/data/app/~~_ONPenk8dLGLa3bFJVgmjg==/com.miHoYo.Yuanshen-HU10quAflWxuUB6-bLtjxA==/lib/arm64/libMmoron.so
(CAKAAudioBackend::OnAudioReady(AAudioStreamStruct, void*, int)+192) (BuildId: c94f76a9baa34f596e39c45d05e918c4f77834ff)
06-28 16:23:06.393 2154 2154 F DEBUG : #02 pc 0000000000022428 /system/lib64/libaudio_internal.so (aaudio::AudioStream::maybeCallDataCallback(void*,
int)+196) (BuildId: 66808d41f3a1a8f39cf256d62733487b)
06-28 16:23:06.393 2154 2154 F DEBUG : #03 pc 0000000000024d04 /system/lib64/libaudio_internal.so
(aaudio::AudioStreamLegacy::callDataCallbackFrames(unsigned char*, int)+308) (BuildId: 66808d41f3a1a8f39cf256d62733487b)
06-28 16:23:06.393 2154 2154 F DEBUG : #04 pc 0000000000025488 /system/lib64/libaudio_internal.so (aaudio::AudioStreamLegacy::processCallbackCommon(int,
void*))+752) (BuildId: 66808d41f3a1a8f39cf256d62733487b)
06-28 16:23:06.393 2154 2154 F DEBUG : #05 pc 000000000008cbc4 /system/lib64/libaudioclient.so (android::AudioTrack::processAudioBuffer()+2368) (BuildId:
7e2fd052f094400631569a2bbd95426f)
06-28 16:23:06.393 2154 2154 F DEBUG : #06 pc 000000000008bf84 /system/lib64/libaudioclient.so (android::AudioTrack::AudioTrackThread::threadLoop()+288)
(BuildId: 7e2fd052f094400631569a2bbd95426f)
06-28 16:23:06.393 2154 2154 F DEBUG : #07 pc 0000000000013654 /system/lib64/libutils.so (android::Thread::_threadLoop(void*))+464) (BuildId:
b940f836006eead456c936e97e64d2d4)
06-28 16:23:06.393 2154 2154 F DEBUG : #08 pc 00000000000bd47c /system/lib64/libandroid_runtime.so (android::AndroidRuntime::javaThreadShell(void*))+148)
(BuildId: 3a68524b7a6d7f6ccfcfc32def7d4f64)
06-28 16:23:06.393 2154 2154 F DEBUG : #09 pc 0000000000012de8 /system/lib64/libutils.so (thread_data_t::trampoline(thread_data_t const*))+408) (BuildId:
b940f836006eead456c936e97e64d2d4)
06-28 16:23:06.393 2154 2154 F DEBUG : #10 pc 00000000000b6a24 /apex/com.android.runtime/lib64/bionic/libc.so (_pthread_start(void*))+264) (BuildId:
369edc656806aeaf384cbeb8f7a347af)
06-28 16:23:06.393 2154 2154 F DEBUG : #11 pc 00000000000532bc /apex/com.android.runtime/lib64/bionic/libc.so (_start_thread+68) (BuildId:
369edc656806aeaf384cbeb8f7a347af)
-----
```

#2 - 2023-06-29 10:13 - Multimedia组-RD3_TSCD 梁卿山

- Status changed from New to RESOLVED
- Resolution changed from -- to WONTFIX

Hi ALL

从上面的堆栈信息分析：
发生奔溃的原因是APP内存空指针了，null pointer dereference；

```
06-28 16:23:06.393 2154 2154 F DEBUG : #00 pc 00000000001dae34
/data/app/~~_ONPenk8dLGLa3bFJVgmjg==/com.miHoYo.Yuanshen-HU10quAflWxuUB6-bLtjxA==/lib/arm64/libMmoron.so
```

(CAkSink::OnIncompleteWrite(unsigned int)+44) (BuildId: c94f76a9baa34f596e39c45d05e918c4f77834ff)应用内接口

06-28 16:23:06.393 2154 2154 F DEBUG : #01 pc 00000000001ff91c

/data/app/~~_0NPenk8dLGLa3bFJVgmjg==/com.miHoYo.Yuanshen-HU10quAflWxuUB6-bLtjxA==/lib/arm64/libMmoron.so

(CAkAAudioBackend::OnAudioReady(AAudioStreamStruct, void*, int)+192) (BuildId: c94f76a9baa34f596e39c45d05e918c4f77834ff)应用内接口

06-28 16:23:06.393 2154 2154 F DEBUG : #02 pc 0000000000022428 /system/lib64/libaaudio_internal.so (aaudio::AudioStream::maybeCallDataCallback(void*,

int)+196) (BuildId: 66808d41f3a1a8f39cf256d62733487b)安卓原生接口

06-28 16:23:06.393 2154 2154 F DEBUG : #03 pc 0000000000024d04 /system/lib64/libaaudio_internal.so

(aaudio::AudioStreamLegacy::callDataCallbackFrames(unsigned char*, int)+308) (BuildId: 66808d41f3a1a8f39cf256d62733487b)

06-28 16:23:06.393 2154 2154 F DEBUG : #04 pc 0000000000025488 /system/lib64/libaaudio_internal.so

(aaudio::AudioStreamLegacy::processCallbackCommon(int, void*)+752) (BuildId: 66808d41f3a1a8f39cf256d62733487b)

06-28 16:23:06.393 2154 2154 F DEBUG : #05 pc 000000000008cbc4 /system/lib64/libaudioclient.so (android::AudioTrack::processAudioBuffer()+2368) (BuildId:

7e2fd052f094400631569a2bbd95426f)

06-28 16:23:06.393 2154 2154 F DEBUG : #06 pc 000000000008bf84 /system/lib64/libaudioclient.so

(android::AudioTrack::AudioTrackThread::threadLoop()+288) (BuildId: 7e2fd052f094400631569a2bbd95426f)

总结：

原生使用的是原生的aaudio API进行音频的相关操作，

aaudio 通过maybeCallDataCallback回调到应用内部时，应用内部出现了空指针，导致了应用的crash。

该问题是应用问题。

#3 - 2023-08-24 17:12 - CDTs_TEST 王成

- Status changed from RESOLVED to ASSIGNED

麻烦标注Root cause 后回转BUG

Files			
6.mp4	18.4 MB	2023-06-28	物联网测试组_TSCD 王维
6.txt	8.49 MB	2023-06-28	物联网测试组_TSCD 王维