

Figure - Bug #118738

【AF】【EVT3】【实车】10：14左右 重新整车上电后 副屏卡顿TP无效 约卡顿一分钟左右自动重启

2023-06-12 10:49 - CD TEST-方永红

Status:	ASSIGNED	Start date:	2023-06-12
Priority:	Urgent	Due date:	
Assignee:	CD BSP-余霄	% Done:	0%
Category:	BSP	Estimated time:	0.00 hour
Target version:			
Need_Info:	--	Found Version:	0106
Resolution:	--	Degrated:	--
Severity:	Critical	Verified Version:	
Reproducibility:	Occasionally	Fixed Version:	
Test Type:	ST	Root cause:	
Description			
【测试环境】 实车测试			
【测试版本】 0106			
【问题描述】 10：14左右 重新整车上电后 副屏卡顿TP无效 约卡顿一分钟左右自动重启			
Subtasks:			
Bug # 118743: 【AF】【EVT3】【实车】10：14左右 重新整车上电后 副屏卡顿TP无效 约卡顿一分钟左右自动重启			New

History

#1 - 2023-06-12 10:52 - CD TEST-方永红

ftp://cdiot@192.168.87.46/Pre_figure/Test_Log/118738

#2 - 2023-06-12 14:36 - CD FW 曹覃刚

- Status changed from New to ASSIGNED
- Assignee changed from CD FW 曹覃刚 to CD FW 郑雷

■ 我的分析

从日志看，重启了两次

anr_2023-06-12-10-09-32-980

anr_2023-06-12-10-10-15-146

"PowerManagerService" prio=5 tid=36 Native | group="main" sCount=1 ucsCount=0 flags=1 obj=0x156023d0 self=0xb4000072206412e0 | sysTid=1708 nice=-4
cgrp=default sched=0/0 handle=0x7007a32cb0 | state=S schedstat=(55161504 109276879 745) utm=1 stm=4 core=0 HZ=100 | stack=0x700792f000-0x7007931000
stackSize=1039KB | held mutexes=
native: #00 pc 00000000000a1c88 /apex/com.android.runtime/lib64/bionic/libc.so (__ioctl+8)
native: #01 pc 0000000000005b8d4 /apex/com.android.runtime/lib64/bionic/libc.so (ioctl+156)
native: #02 pc 00000000000053070 /system/lib64/libbinder.so (android::IPCThreadState::talkWithDriver(bool)+292)
native: #03 pc 000000000000542e4 /system/lib64/libbinder.so (android::IPCThreadState::waitForResponse(android::Parcel*, int*)+120)
native: #04 pc 00000000000053ff0 /system/lib64/libbinder.so (android::IPCThreadState::transact(int, unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+224)
native: #05 pc 0000000000004bafc /system/lib64/libbinder.so (android::BpBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+196)

```
native: #06 pc 0000000000c6fd0 /system/lib64/libgui.so (android::BpSurfaceComposer::captureDisplay(android::DisplayCaptureArgs const&,
android::sp<android::gui::IScreenCaptureListener> const&)+476)
native: #07 pc 0000000000f72a0 /system/lib64/libgui.so (android::ScreenshotClient::captureDisplay(android::DisplayCaptureArgs const&,
android::sp<android::gui::IScreenCaptureListener> const&)+80)
native: #08 pc 000000000131f4c /system/lib64/libandroid_runtime.so (android::nativeCaptureDisplay(_JNIEnv*, _jclass*, _jobject*, _jobject*)+540)
at android.view.SurfaceControl.nativeCaptureDisplay(Native method)
at android.view.SurfaceControl.captureDisplay(SurfaceControl.java:2300)
at android.view.SurfaceControl.captureDisplay(SurfaceControl.java:2312)
at com.android.server.display.DisplayManagerService.systemScreenshotInternal(DisplayManagerService.java:1647)
- locked <0x0a0bd0e3> (a com.android.server.display.DisplayManagerService$SyncRoot)
at com.android.server.display.DisplayManagerService.access$6200(DisplayManagerService.java:185)
at com.android.server.display.DisplayManagerService$LocalService.systemScreenshot(DisplayManagerService.java:3165)
at com.android.server.display.ColorFade.captureScreen(ColorFade.java:558)
at com.android.server.display.ColorFade.prepare(ColorFade.java:178)
at com.android.server.display.DisplayPowerState.prepareColorFade(DisplayPowerState.java:227)
at com.android.server.display.DisplayPowerController.animateScreenStateChange(DisplayPowerController.java:1897)
at com.android.server.display.DisplayPowerController.updatePowerState(DisplayPowerController.java:1114)
at com.android.server.display.DisplayPowerController.access$700(DisplayPowerController.java:97)
at com.android.server.display.DisplayPowerController$DisplayControllerHandler.handleMessage(DisplayPowerController.java:2404)
at android.os.Handler.dispatchMessage(Handler.java:106)
at android.os.Looper.loopOnce(Looper.java:201)
at android.os.Looper.loop(Looper.java:288)
at android.os.HandlerThread.run(HandlerThread.java:67)
at com.android.server.ServiceThread.run(ServiceThread.java:44)
```

06-12 10:10:22.287 1561 1631 W Watchdog: *** WATCHDOG KILLING SYSTEM PROCESS: Blocked in monitor com.android.server.power.PowerManagerService on foreground thread (android.fg), Blocked in handler on main thread (main), Blocked in handler on PowerManagerService (PowerManagerService)

//第一次重启, block在PowerManagerService

anr_2023-06-12-10-11-24-523

anr_2023-06-12-10-11-58-328

anr_2023-06-12-10-13-10-648

"main" prio=5 tid=1 Sleeping | group="main" sCount=1 ucsCount=0 flags=1 obj=0x7144b078 self=0xb4000079d29dc7b0 | sysTid=9076 nice=-2 cgrp=default sched=0/0
handle=0x7ba28614f8 | state=S schedstat=(1282160011 17707678208 2695) utm=103 stm=24 core=1 HZ=100 | stack=0x7fed208000-0x7fed20a000 stackSize=8188KB |
held mutexes=

```
at java.lang.Thread.sleep(Native method)
- sleeping on <0x07a6ff1b> (a java.lang.Object)
at java.lang.Thread.sleep(Thread.java:451)
- locked <0x07a6ff1b> (a java.lang.Object)
at java.lang.Thread.sleep(Thread.java:356)
at android.net.util.NetdService.get(NetdService.java:96)
at android.net.util.NetdService.get(NetdService.java:114)
at com.android.server.NetworkManagementService$Dependencies.getNetd(NetworkManagementService.java:127)
at com.android.server.NetworkManagementService.connectNativeNetdService(NetworkManagementService.java:432)
at com.android.server.NetworkManagementService.create(NetworkManagementService.java:265)
at com.android.server.NetworkManagementService.create(NetworkManagementService.java:271)
at com.android.server.SystemServer.startOtherServices(SystemServer.java:1813)
at com.android.server.SystemServer.run(SystemServer.java:885)
at com.android.server.SystemServer.main(SystemServer.java:616)
at java.lang.reflect.Method.invoke(Native method)
at com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run(RuntimeInit.java:548)
at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:987)
```

06-12 10:12:09.314 9076 9099 W Watchdog: *** WATCHDOG KILLING SYSTEM PROCESS: Blocked in handler on main thread (main)

//第二次重启

■ 下一步计划

1.解析PowerManagerService block的原因

2.LC的同学看看 NetdService sleep, 导致system_server主进程阻塞的原因 #118743

#3 - 2023-06-12 16:45 - CD FW 郑雷

- Category changed from CD-FW to BSP

- Assignee changed from CD FW 郑雷 to CD BSP- 杜磊

[当前分析]

1.关于Watchdog: *** WATCHDOG KILLING SYSTEM PROCESS: Blocked in monitor com.android.server.power.PowerManagerService on foreground thread (android.fg), Blocked in handler on main thread (main), Blocked in handler on PowerManagerService (PowerManagerService)的分析。

06-12 10:10:22.180 1561 1631 E Watchdog: First set of traces taken from /data/anr/anr_2023-06-12-10-09-32-980

06-12 10:10:22.220 1561 1631 E Watchdog: Second set of traces taken from /data/anr/anr_2023-06-12-10-10-15-146

06-12 10:10:22.268 1561 8969 I DropBoxManagerService: add tag=system_server_watchdog isTagEnabled=true flags=0x6

06-12 10:10:22.283 2107 2107 D MicroService: onHeartBeatDetected

06-12 10:10:22.283 2107 2107 D MicroService: sendHeartbeatMessage

06-12 10:10:22.287 1561 1631 W Watchdog: * WATCHDOG KILLING SYSTEM PROCESS: Blocked in monitor com.android.server.power.PowerManagerService on foreground thread (android.fg), Blocked in handler on main thread (main), Blocked in handler on PowerManagerService (PowerManagerService)

06-12 10:10:22.287 1561 1631 W Watchdog: android.fg annotated stack trace:

06-12 10:10:22.287 1561 1631 W Watchdog: at com.android.server.power.PowerManagerService.monitor(PowerManagerService.java:4124)

06-12 10:10:22.288 1561 1631 W Watchdog: - waiting to lock <0x0423ac08> (a java.lang.Object)

06-12 10:10:22.288 1561 1631 W Watchdog: at com.android.server.Watchdog\$HandlerChecker.run(Watchdog.java:275)

06-12 10:10:22.288 1561 1631 W Watchdog: at android.os.Handler.handleCallback(Handler.java:938)

06-12 10:10:22.288 1561 1631 W Watchdog: at android.os.Handler.dispatchMessage(Handler.java:99)

06-12 10:10:22.288 1561 1631 W Watchdog: at android.os.Looper.loopOnce(Looper.java:201)

06-12 10:10:22.288 1561 1631 W Watchdog: at android.os.Looper.loop(Looper.java:288)

06-12 10:10:22.288 1561 1631 W Watchdog: at android.os.HandlerThread.run(HandlerThread.java:67)

06-12 10:10:22.288 1561 1631 W Watchdog: at com.android.server.ServiceThread.run(ServiceThread.java:44)

06-12 10:10:22.288 1561 1631 W Watchdog: main annotated stack trace:

06-12 10:10:22.288 1561 1631 W Watchdog: at com.android.server.alarm.AlarmManagerService\$DeliveryTracker.alarmComplete(AlarmManagerService.java:4835)

06-12 10:10:22.289 1561 1631 W Watchdog: - waiting to lock <0x0957b286> (a java.lang.Object)

06-12 10:10:22.289 1561 1631 W Watchdog: at

com.android.server.alarm.AlarmManagerService\$3.lambda\$doAlarm\$0\$AlarmManagerService\$3(AlarmManagerService.java:1684)

06-12 10:10:22.289 1561 1631 W Watchdog: at com.android.server.alarm.AlarmManagerService\$3\$ExternalSyntheticLambda0.run(Unknown Source:4)

06-12 10:10:22.289 1561 1631 W Watchdog: at android.os.Handler.handleCallback(Handler.java:938)

06-12 10:10:22.289 1561 1631 W Watchdog: at android.os.Handler.dispatchMessage(Handler.java:99)

06-12 10:10:22.289 1561 1631 W Watchdog: at android.os.Looper.loopOnce(Looper.java:201)

06-12 10:10:22.289 1561 1631 W Watchdog: at android.os.Looper.loop(Looper.java:288)

06-12 10:10:22.289 1561 1631 W Watchdog: at com.android.server.SystemServer.run(SystemServer.java:909)

06-12 10:10:22.289 1561 1631 W Watchdog: at com.android.server.SystemServer.main(SystemServer.java:616)

06-12 10:10:22.289 1561 1631 W Watchdog: at java.lang.reflect.Method.invoke(Native Method)

06-12 10:10:22.289 1561 1631 W Watchdog: at com.android.internal.os.RuntimeInit\$MethodAndArgsCaller.run(RuntimeInit.java:548)

06-12 10:10:22.289 1561 1631 W Watchdog: at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:987)

06-12 10:10:22.292 1561 1631 W Watchdog: PowerManagerService annotated stack trace:

06-12 10:10:22.292 1561 1631 W Watchdog: at android.view.SurfaceControl.nativeCaptureDisplay(Native Method)

06-12 10:10:22.292 1561 1631 W Watchdog: at android.view.SurfaceControl.captureDisplay(SurfaceControl.java:2300)

06-12 10:10:22.292 1561 1631 W Watchdog: at android.view.SurfaceControl.captureDisplay(SurfaceControl.java:2312)

```

06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.DisplayManagerService.systemScreenshotInternal(DisplayManagerService.java:1647)
06-12 10:10:22.292 1561 1631 W Watchdog: - locked <0x0a0bd0e3> (a com.android.server.display.DisplayManagerService$SyncRoot)
06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.DisplayManagerService.access$6200(DisplayManagerService.java:185)
06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.DisplayManagerService$LocalService.systemScreenshot(DisplayManagerService.java:3165)
06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.ColorFade.captureScreen(ColorFade.java:558)
06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.ColorFade.prepare(ColorFade.java:178)
06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.DisplayPowerState.prepareColorFade(DisplayPowerState.java:227)
06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.DisplayPowerController.animateScreenStateChange(DisplayPowerController.java:1897)
06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.DisplayPowerController.updatePowerState(DisplayPowerController.java:1114)
06-12 10:10:22.292 1561 1631 W Watchdog: at com.android.server.display.DisplayPowerController.access$700(DisplayPowerController.java:97)
06-12 10:10:22.292 1561 1631 W Watchdog: at
com.android.server.display.DisplayPowerController$DisplayControllerHandler.handleMessage(DisplayPowerController.java:2404)
06-12 10:10:22.292 1561 1631 W Watchdog: at android.os.Handler.dispatchMessage(Handler.java:106)
06-12 10:10:22.293 1561 1631 W Watchdog: at android.os.Looper.loopOnce(Looper.java:201)
06-12 10:10:22.293 1561 1631 W Watchdog: at android.os.Looper.loop(Looper.java:288)
06-12 10:10:22.293 1561 1631 W Watchdog: at android.os.HandlerThread.run(HandlerThread.java:67)
06-12 10:10:22.293 1561 1631 W Watchdog: at com.android.server.ServiceThread.run(ServiceThread.java:44)
06-12 10:10:22.293 1561 1631 W Watchdog: * GOODBYE!
06-12 10:10:22.293 1561 1631 I Process : Sending signal. PID: 1561 SIG: 9

```

从anr_2023-06-12-10-09-32-980、anr_2023-06-12-10-10-15-146、traces_SystemServer_WDT12_06_10_10_22.179_pid1561看，都是PowerManagerService的前台线程android.fg被block

。

调用堆栈：

```

"android.fg" prio=5 tid=11 Blocked | group="main" sCount=1 ucsCount=0 flags=1 obj=0x15600fb8 self=0xb400007220619330 | sysTid=1624 nice=0 cgrp=default
sched=0/0 handle=0x70224eecb0 | state=S schedstat=( 206118731 296311971 1017 ) utm=16 stm=3 core=2 HZ=100 | stack=0x70223eb000-0x70223ed000
stackSize=1039KB | held mutexes=
at com.android.server.power.PowerManagerService.monitor(PowerManagerService.java:4124)
- waiting to lock <0x0423ac08> (a java.lang.Object) held by thread 58
at com.android.server.Watchdog$HandlerChecker.run(Watchdog.java:275)
at android.os.Handler.handleCallback(Handler.java:938)
at android.os.Handler.dispatchMessage(Handler.java:99)
at android.os.Looper.loopOnce(Looper.java:201)
at android.os.Looper.loop(Looper.java:288)
at android.os.HandlerThread.run(HandlerThread.java:67)
at com.android.server.ServiceThread.run(ServiceThread.java:44)

```

看门狗线程要去获取0x0423ac08锁来检测PowerManagerService是否阻塞，但是0x0423ac08锁被thread 58持有。

```

"AlarmManager" prio=5 tid=58 Blocked | group="main" sCount=1 ucsCount=0 flags=1 obj=0x14c42808 self=0xb40000722064f160 | sysTid=1809 nice=0 cgrp=default
sched=0/0 handle=0x6ff4ec8cb0 | state=S schedstat=( 22884789 16344482 92 ) utm=1 stm=0 core=1 HZ=100 | stack=0x6ff4dc5000-0x6ff4dc7000 stackSize=1039KB |
held mutexes=
at com.android.server.display.DisplayManagerService$LocalService.requestPowerState(DisplayManagerService.java:3119)
- waiting to lock <0x0a0bd0e3> (a com.android.server.display.DisplayManagerService$SyncRoot) held by thread 36
at com.android.server.power.PowerManagerService.updateDisplayPowerStateLocked(PowerManagerService.java:3203)
at com.android.server.power.PowerManagerService.updatePowerStateLocked(PowerManagerService.java:2159)
at com.android.server.power.PowerManagerService.acquireWakeLockInternal(PowerManagerService.java:1417)
- locked <0x0423ac08> (a java.lang.Object)
at com.android.server.power.PowerManagerService.access$4600(PowerManagerService.java:139)
at com.android.server.power.PowerManagerService$BinderService.acquireWakeLock(PowerManagerService.java:5175)
at android.os.PowerManager$WakeLock.acquireLocked(PowerManager.java:2720)
at android.os.PowerManager$WakeLock.acquire(PowerManager.java:2686)
- locked <0x033f4ae0> (a android.os.Binder)

```

```
at com.android.server.alarm.AlarmManagerService$DeliveryTracker.deliverLocked(AlarmManagerService.java:4968)
at com.android.server.alarm.AlarmManagerService.deliverAlarmsLocked(AlarmManagerService.java:4006)
at com.android.server.alarm.AlarmManagerService$AlarmThread.run(AlarmManagerService.java:4251)
- locked <0x0957b286> (a java.lang.Object)
```

thread 58又在等待0x0a0bd0e3锁，0x0a0bd0e3被thread 36持有。

```
"PowerManagerService" prio=5 tid=36 Native | group="main" sCount=1 ucsCount=0 flags=1 obj=0x156023d0 self=0xb4000072206412e0 | sysTid=1708 nice=-4
cgrp=default sched=0/0 handle=0x7007a32cb0 | state=S schedstat=( 55161504 109276879 745 ) utm=1 stm=4 core=0 HZ=100 | stack=0x700792f000-0x7007931000
stackSize=1039KB | held mutexes=
native: #00 pc 00000000000a1c88 /apex/com.android.runtime/lib64/bionic/libc.so (__ioctl+8)
native: #01 pc 000000000005b8d4 /apex/com.android.runtime/lib64/bionic/libc.so (ioctl+156)
native: #02 pc 0000000000053070 /system/lib64/libbinder.so (android::IPCThreadState::talkWithDriver(bool)+292)
native: #03 pc 00000000000542e4 /system/lib64/libbinder.so (android::IPCThreadState::waitForResponse(android::Parcel*, int*)+120)
native: #04 pc 0000000000053ff0 /system/lib64/libbinder.so (android::IPCThreadState::transact(int, unsigned int, android::Parcel const&, android::Parcel*, unsigned
int)+224)
native: #05 pc 000000000004bafc /system/lib64/libbinder.so (android::BpBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+196)
native: #06 pc 00000000000c6fd0 /system/lib64/libgui.so (android::BpSurfaceComposer::captureDisplay(android::DisplayCaptureArgs const&,
android::sp<android::gui::IScreenCaptureListener> const&)+476)
native: #07 pc 00000000000f72a0 /system/lib64/libgui.so (android::ScreenshotClient::captureDisplay(android::DisplayCaptureArgs const&,
android::sp<android::gui::IScreenCaptureListener> const&)+80)
native: #08 pc 0000000000131f4c /system/lib64/libandroid_runtime.so (android::nativeCaptureDisplay(_JNIEnv*, _jclass*, _jobject*, _jobject*)+540)
at android.view.SurfaceControl.nativeCaptureDisplay(Native method)
at android.view.SurfaceControl.captureDisplay(SurfaceControl.java:2300)
at android.view.SurfaceControl.captureDisplay(SurfaceControl.java:2312)
at com.android.server.display.DisplayManagerService.systemScreenshotInternal(DisplayManagerService.java:1647)
- locked <0x0a0bd0e3> (a com.android.server.display.DisplayManagerService$SyncRoot)
at com.android.server.display.DisplayManagerService.access$6200(DisplayManagerService.java:185)
at com.android.server.display.DisplayManagerService$LocalService.systemScreenshot(DisplayManagerService.java:3165)
at com.android.server.display.ColorFade.captureScreen(ColorFade.java:558)
at com.android.server.display.ColorFade.prepare(ColorFade.java:178)
at com.android.server.display.DisplayPowerState.prepareColorFade(DisplayPowerState.java:227)
at com.android.server.display.DisplayPowerController.animateScreenStateChange(DisplayPowerController.java:1897)
at com.android.server.display.DisplayPowerController.updatePowerState(DisplayPowerController.java:1114)
at com.android.server.display.DisplayPowerController.access$700(DisplayPowerController.java:97)
at com.android.server.display.DisplayPowerController$DisplayControllerHandler.handleMessage(DisplayPowerController.java:2404)
at android.os.Handler.dispatchMessage(Handler.java:106)
at android.os.Looper.loopOnce(Looper.java:201)
at android.os.Looper.loop(Looper.java:288)
at android.os.HandlerThread.run(HandlerThread.java:67)
at com.android.server.ServiceThread.run(ServiceThread.java:44)
```

从thread 36的堆栈看，它正在执行binder调用到SurfaceFlinger进程。接下来看下SurfaceFlinger进程的信息。

```
----- pid 984 at 2023-06-12 10:10:16.167425670+0800 -----
Cmd line: /system/bin/surfaceflinger
ABI: 'arm64'
```

```
"surfaceflinger" sysTid=984
#00 pc 00000000000a2c4c /apex/com.android.runtime/lib64/bionic/libc.so (_epoll_pwait+12) (BuildId: 369edc656806aeaf384cbeb8f7a347af)
#01 pc 0000000000017ea8 /system/lib64/libutils.so (android::Looper::pollInner(int)+184) (BuildId: b940f836006eead456c936e97e64d2d4)
#02 pc 0000000000017d84 /system/lib64/libutils.so (android::Looper::pollOnce(int, int*, int*, void**)+116) (BuildId: b940f836006eead456c936e97e64d2d4)
#03 pc 000000000016f870 /system/bin/surfaceflinger (android::impl::MessageQueue::waitMessage()+88) (BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)
```

#04 pc 0000000001891d4 /system/bin/surfaceflinger (android::SurfaceFlinger::run()+100) (BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)

#05 pc 00000000001d7248 /system/bin/surfaceflinger (main+1640) (BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)

#06 pc 000000000004a084 /apex/com.android.runtime/lib64/bionic/libc.so (_libc_init+100) (BuildId: 369edc656806aeaf384cbeb8f7a347af)

"Binder:984_1" sysTid=1097

#00 pc 0000000000a1c88 /apex/com.android.runtime/lib64/bionic/libc.so (_ioctl+8) (BuildId: 369edc656806aeaf384cbeb8f7a347af)

#01 pc 000000000005b8d4 /apex/com.android.runtime/lib64/bionic/libc.so (ioctl+156) (BuildId: 369edc656806aeaf384cbeb8f7a347af)

#02 pc 0000000000066b40 /system/lib64/libhidlbase.so (android::hardware::IPCThreadState::transact(int, unsigned int, android::hardware::Parcel const&, android::hardware::Parcel*, unsigned int)+1540) (BuildId: c608f6971797e3ae95b93820aa139249)

#03 pc 0000000000066bdc /system/lib64/libhidlbase.so (android::hardware::BpHwBinder::transact(unsigned int, android::hardware::Parcel const&, android::hardware::Parcel*, unsigned int, std::__1::function<void (android::hardware::Parcel&)>)+80) (BuildId: c608f6971797e3ae95b93820aa139249)

#04 pc 000000000011354 /system/lib64/[android.hardware.graphics.allocator@3.0.so](#)
(android::hardware::graphics::allocator::V3_0::BpHwAllocator::_hidl_allocate(android::hardware::IInterface*, android::hardware::details::HidlInstrumentor*, android::hardware::hidl_vec<unsigned int> const&, unsigned int, std::__1::function<void (android::hardware::graphics::mapper::V3_0::Error, unsigned int, android::hardware::hidl_vec<android::hardware::hidl_handle> const&)>) (c.f.)+432) (BuildId: 9e99b70c76edd0355585529c53ae3c9)

#05 pc 000000000010b9c /system/lib64/[android.hardware.graphics.allocator@3.0.so](#)
(android::hardware::graphics::allocator::V3_0::BpHwAllocator::allocate(android::hardware::hidl_vec<unsigned int> const&, unsigned int, std::__1::function<void (android::hardware::graphics::mapper::V3_0::Error, unsigned int, android::hardware::hidl_vec<android::hardware::hidl_handle> const&)>)+168) (BuildId: 9e99b70c76edd0355585529c53ae3c9)

#06 pc 000000000002d5b8 /system/lib64/libui.so (android::Gralloc3Allocator::allocate(std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char>>, unsigned int, unsigned int, int, unsigned int, unsigned long, unsigned int, unsigned int*, native_handle const**, bool) const+224) (BuildId: 340f577d9dcac1454a4c9b79cdd3f91a)

#07 pc 00000000000380c8 /system/lib64/libui.so (android::GraphicBufferAllocator::allocateHelper(unsigned int, unsigned int, int, unsigned int, unsigned long, native_handle const**, unsigned int*, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char>>, bool)+320) (BuildId: 340f577d9dcac1454a4c9b79cdd3f91a)

#08 pc 00000000000384e0 /system/lib64/libui.so (android::GraphicBufferAllocator::allocate(unsigned int, unsigned int, int, unsigned int, unsigned long, native_handle const**, unsigned int*, unsigned long, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char>>)+140) (BuildId: 340f577d9dcac1454a4c9b79cdd3f91a)

#09 pc 0000000000036188 /system/lib64/libui.so (android::GraphicBuffer::initWithSize(unsigned int, unsigned int, int, unsigned int, unsigned long, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char>>)+216) (BuildId: 340f577d9dcac1454a4c9b79cdd3f91a)

#10 pc 0000000000036060 /system/lib64/libui.so (android::GraphicBuffer::GraphicBuffer(unsigned int, unsigned int, int, unsigned int, unsigned long, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char>>)+128) (BuildId: 340f577d9dcac1454a4c9b79cdd3f91a)

#11 pc 00000000001cbd48 /system/bin/surfaceflinger (android::surfaceflinger::DefaultFactory::createGraphicBuffer(unsigned int, unsigned int, int, unsigned int, unsigned long, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char>>)+128) (BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)

#12 pc 00000000001acf4c /system/bin/surfaceflinger (android::SurfaceFlinger::captureScreenCommon(std::__1::future<std::__1::unique_ptr<android::RenderArea, std::__1::default_delete<android::RenderArea>>>, std::__1::function<void (std::__1::function<void (android::Layer*)> const&)>, android::ui::Size, android::hardware::graphics::common::V1_2::PixelFormat, bool, bool, android::sp<android::gui::IScreenCaptureListener> const&)+968) (BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)

#13 pc 00000000001aca00 /system/bin/surfaceflinger (android::SurfaceFlinger::captureDisplay(android::DisplayCaptureArgs const&, android::sp<android::gui::IScreenCaptureListener> const&)+2020) (BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)

#14 pc 0000000000c31d0 /system/lib64/libgui.so (android::BnSurfaceComposer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+8828) (BuildId: 448b4199bacacf9417cd93df4f7390f5)

#15 pc 00000000001aa5c8 /system/bin/surfaceflinger (android::SurfaceFlinger::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+852) (BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)

#16 pc 0000000000049880 /system/lib64/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+252) (BuildId: 07bc4d4147790b1e0ac44f7625168f4a)

#17 pc 00000000000538cc /system/lib64/libbinder.so (android::IPCThreadState::executeCommand(int)+1048) (BuildId: 07bc4d4147790b1e0ac44f7625168f4a)

#18 pc 00000000000533e8 /system/lib64/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+164) (BuildId: 07bc4d4147790b1e0ac44f7625168f4a)

#19 pc 0000000000053c98 /system/lib64/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+72) (BuildId: 07bc4d4147790b1e0ac44f7625168f4a)

#20 pc 0000000000080484 /system/lib64/libbinder.so (android::PoolThread::threadLoop()+28) (BuildId: 07bc4d4147790b1e0ac44f7625168f4a)

#21 pc 00000000001358c /system/lib64/libutils.so (android::Thread::_threadLoop(void*)+264) (BuildId: b940f83600eead456c936e97e64d2d4)

#22 pc 000000000012de8 /system/lib64/libutils.so (thread_data_t::trampoline(thread_data_t const*)+408) (BuildId: b940f83600eead456c936e97e64d2d4)

#23 pc 00000000000b6a24 /apex/com.android.runtime/lib64/bionic/libc.so (_pthread_start(void*)+264) (BuildId: 369edc656806aeaf384cbeb8f7a347af)

#24 pc 00000000000532bc /apex/com.android.runtime/lib64/bionic/libc.so (_start_thread+68) (BuildId: 369edc656806aeaf384cbeb8f7a347af)

从SurfaceFlinger的binder线程Binder:984_1的堆栈看，Binder:984_1在执行captureDisplay方法在申请GraphicBuffer，binder调用到[android.hardware.graphics.allocator@3.0.so](#)的allocate方法，但是没有返回，被block在住了。引起了WATCHDOG异常

[下一步Action]

需要BSP Display team帮忙分析[android.hardware.graphics.allocator@3.0.so](#)的allocate没有返回的原因。

#4 - 2023-06-13 18:07 - CD BSP-杜磊

[android.hardware.graphics.allocator@3.0.so](#) 为高通相关库。

next step:

起case咨询高通

#5 - 2023-06-14 17:18 - CD BSP-杜磊

Qcom Case

06674564

#6 - 2023-06-14 17:34 - CD BSP-杜磊

- Description updated

#7 - 2023-06-14 17:36 - CD BSP-杜磊

- Description updated

#8 - 2023-06-15 15:23 - CD BSP-杜磊

高通回复如下：

How did you copy this issue? from my experience, it should relate to the APP side.
some mis-operation in uplayer will cause this buffer allocator issue. as usual,
if you can figure out where/how this issue occurred within the APP, just remove them to varify.

#9 - 2023-06-20 10:00 - CD BSP-杜磊

- Assignee changed from CD BSP-杜磊 to CD BSP-余霄