

Status:	CLOSED	Start date:	2023-06-07
Priority:	High	Due date:	
Assignee:	CD TEST-方永红	% Done:	100%
Category:	CD-FW	Estimated time:	0.00 hour
Target version:			
Need_Info:	--	Found Version:	0107
Resolution:	DUPLICATE	Degrated:	No
Severity:	Critical	Verified Version:	
Reproducibility:	Rarely	Fixed Version:	
Test Type:	Monkey Test	Root cause:	与 #118327 是同伴问题
Description			
【执行命令】 monkey --pkg-blacklist-file /sdcard/blackList.txt --hprof --throttle 500 -s 1234567 --pct-touch 35 --pct-motion 25 --pct-appswitch 30 --pct-pinchzoom 5 --pct-trackball 0 --pct-anyevent 5 --ignore-crashes --ignore-timeouts --ignore-security-exceptions --monitor-native-crashes --ignore-native-crashes --pct-syskeys 0 -v -v -v 12000000 2>/sdcard/error.txt 1>/sdcard/info.txt 【测试结果】 monkey异常停止，设备进入屏保			
Related issues:			
Related to Figure - Bug # 118327: 【AF】【EVT3】【Monkey】Devic...		CLOSED	2023-05-18 2023-06-05

History

#1 - 2023-06-07 10:06 - CD TEST-方永红

ftp://cdiot@192.168.87.46/Pre_figure/Test_Log/118598

- #2 - 2023-06-07 10:31 - CD FW 曹覃刚
- Status changed from New to RESOLVED
 - Assignee changed from CD FW 曹覃刚 to CD TEST-方永红
 - % Done changed from 0 to 100
 - Resolution changed from -- to DUPLICATE
 - Degrated changed from -- to No
 - Root cause set to 与 #118327 是同伴问题

■ 我的分析

surfaceflinger报错，导致system_server重启，高通的libdolphin.so中报出来的问题

与 #118327 是同伴问题，将在#118327中跟踪

06-07 05:18:44.374 29762 29762 F DEBUG : Build fingerprint: 'HiPhi/PassengerDisplay_CN/PassengerDisplay:12/SKQ1.220201.001/3830:user/test-keys'

06-07 05:18:44.374 29762 29762 F DEBUG : Revision: '0'

06-07 05:18:44.374 29762 29762 F DEBUG : ABI: 'arm64'

06-07 05:18:44.374 29762 29762 F DEBUG : Timestamp: 2023-06-07 05:18:43.647389874+0800

06-07 05:18:44.374 29762 29762 F DEBUG : Process uptime: 29920s

06-07 05:18:44.374 29762 29762 F DEBUG : Cmdline: /system/bin/surfaceflinger

06-07 05:18:44.374 29762 29762 F DEBUG : pid: 993, tid: 1710, name: Binder:993_4 >>> /system/bin/surfaceflinger <<<

```

06-07 05:18:44.374 29762 29762 F DEBUG : uid: 1000
06-07 05:18:44.374 29762 29762 F DEBUG : signal 6 (SIGABRT), code 1 (SI_QUEUE), fault addr -----
06-07 05:18:44.374 29762 29762 F DEBUG : Abort message: 'Scudo ERROR: invalid chunk state when deallocating address 0x2000077653f24f0
06-07 05:18:44.374 29762 29762 F DEBUG : '
06-07 05:18:44.374 29762 29762 F DEBUG : x0 0000000000000000 x1 000000000000006ae x2 0000000000000006 x3 00000076f32cdba0
06-07 05:18:44.374 29762 29762 F DEBUG : x4 0000000000808080 x5 0000000000808080 x6 0000000000808080 x7 8080800000000000
06-07 05:18:44.374 29762 29762 F DEBUG : x8 00000000000000f0 x9 85645764796add7b x10 0000000000000000 x11 fffff80ffffffdf
06-07 05:18:44.374 29762 29762 F DEBUG : x12 0000000000000001 x13 00000085cbdf18ff x14 001fb5acead0f400 x15 0000000000000070
06-07 05:18:44.374 29762 29762 F DEBUG : x16 0000007a17453060 x17 0000007a1742f560 x18 00000076edb70000 x19 000000000000003e1
06-07 05:18:44.374 29762 29762 F DEBUG : x20 000000000000006ae x21 00000000ffffff x22 0000000000000000 x23 b4000077652f2890
06-07 05:18:44.374 29762 29762 F DEBUG : x24 0000007a237b1000 x25 00000076f32cde38 x26 00000076f32ce270 x27 00000076f32ce1d8
06-07 05:18:44.375 29762 29762 F DEBUG : x28 00000076f32cdf0 x29 00000076f32cdc20
06-07 05:18:44.375 29762 29762 F DEBUG : lr 0000007a173df95c sp 00000076f32cdb80 pc 0000007a173df988 pst 0000000000001000
06-07 05:18:44.375 29762 29762 F DEBUG : backtrace:
06-07 05:18:44.375 29762 29762 F DEBUG : #00 pc 0000000000051988 /apex/com.android.runtime/lib64/bionic/libc.so (abort+168) (BuildId:
369edc656806aeaf384cbeb8f7a347af)
06-07 05:18:44.375 29762 29762 F DEBUG : #01 pc 000000000004165c /apex/com.android.runtime/lib64/bionic/libc.so (scudo::die()+12) (BuildId:
369edc656806aeaf384cbeb8f7a347af)
06-07 05:18:44.375 29762 29762 F DEBUG : #02 pc 0000000000041d74 /apex/com.android.runtime/lib64/bionic/libc.so
(scudo::ScopedErrorReport::~ScopedErrorReport()+36) (BuildId: 369edc656806aeaf384cbeb8f7a347af)
06-07 05:18:44.375 29762 29762 F DEBUG : #03 pc 0000000000041fc8 /apex/com.android.runtime/lib64/bionic/libc.so
(scudo::reportInvalidChunkState(scudo::AllocatorAction, void*)+80) (BuildId: 369edc656806aeaf384cbeb8f7a347af)
06-07 05:18:44.375 29762 29762 F DEBUG : #04 pc 0000000000043664 /apex/com.android.runtime/lib64/bionic/libc.so (scudo::Allocator<scudo::AndroidConfig,
&(scudo::_malloc_postinit)>::deallocate(void*, scudo::Chunk::Origin, unsigned long, unsigned long)+316) (BuildId: 369edc656806aeaf384cbeb8f7a347af)
06-07 05:18:44.375 29762 29762 F DEBUG : #05 pc 000000000000aaf4 /system_ext/lib64/libdolphin.so (android::updateLayerListLocked(std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&, bool) (.cfi)+372) (BuildId: a2bd01334f3682675a19bcb37cfc7c99)
06-07 05:18:44.375 29762 29762 F DEBUG : #06 pc 000000000000b3e4 /system_ext/lib64/libdolphin.so (dolphinTrackBufferIncrement.cfi+436) (BuildId:
a2bd01334f3682675a19bcb37cfc7c99)
06-07 05:18:44.375 29762 29762 F DEBUG : #07 pc 00000000001c0bc0 /system/bin/surfaceflinger (ZNSt3
__110__function6__funclZN7android14SurfaceFlinger19setTransactionStateERKNS2_17FrameTimelineInfoERKNS2_6VectorINS2_13ComposerStateEEERKNS7_INS2_
12DisplayStateEEEEjRKNS2_2spINS2_7IBinderEEERKNS2_19InputWindowCommandsElbRKNS2_14client_cache_tEbRKNS2_6vectorINS2_17ListenerCallbacksENS_9a
locatorISS_EEEEEmE$4_65NST_ISY_EEFvRKNS2_13layer_state_tEEECIES12_$8fd14edc326db0e9be510f46fb0c4dd5+688) (BuildId:
9e93e9ccd42ba048dfd020375b5b0dd4)
06-07 05:18:44.375 29762 29762 F DEBUG : #08 pc 00000000001a0e40 /system/bin/surfaceflinger
(android::SurfaceFlinger::setTransactionState(android::FrameTimelineInfo const&, android::Vector<android::ComposerState> const&,
android::Vector<android::DisplayState> const&, unsigned int, android::sp<android::IBinder> const&, android::InputWindowCommands const&, long, bool,
android::client_cache_t const&, bool, std::__1::vector<android::ListenerCallbacks, std::__1::allocator<android::ListenerCallbacks> > const&, unsigned long)+1724)
(BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)
06-07 05:18:44.375 29762 29762 F DEBUG : #09 pc 00000000000c44d8 /system/lib64/libgui.so (android::BnSurfaceComposer::onTransact(unsigned int,
android::Parcel const&, android::Parcel*, unsigned int)+13700) (BuildId: 448b4199bacacf9417cd93df4f7390f5)
06-07 05:18:44.375 29762 29762 F DEBUG : #10 pc 00000000001aa5c8 /system/bin/surfaceflinger (android::SurfaceFlinger::onTransact(unsigned int, android::Parcel
const&, android::Parcel*, unsigned int)+852) (BuildId: 9e93e9ccd42ba048dfd020375b5b0dd4)
06-07 05:18:44.375 29762 29762 F DEBUG : #11 pc 0000000000049880 /system/lib64/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&,
android::Parcel*, unsigned int)+252) (BuildId: 07bc4d4147790b1e0ac44f7625168f4a)
06-07 05:18:44.375 29762 29762 F DEBUG : #12 pc 00000000000538cc /system/lib64/libbinder.so (android::IPCThreadState::executeCommand(int)+1048) (BuildId:
07bc4d4147790b1e0ac44f7625168f4a)
06-07 05:18:44.375 29762 29762 F DEBUG : #13 pc 00000000000533e8 /system/lib64/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+164)
(BuildId: 07bc4d4147790b1e0ac44f7625168f4a)
06-07 05:18:44.375 29762 29762 F DEBUG : #14 pc 0000000000053c98 /system/lib64/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+72) (BuildId:
07bc4d4147790b1e0ac44f7625168f4a)
06-07 05:18:44.375 29762 29762 F DEBUG : #15 pc 0000000000080484 /system/lib64/libbinder.so (android::PoolThread::threadLoop()+28) (BuildId:
07bc4d4147790b1e0ac44f7625168f4a)
06-07 05:18:44.375 29762 29762 F DEBUG : #16 pc 00000000001358c /system/lib64/libutils.so (android::Thread::_threadLoop(void*)+264) (BuildId:

```

b940f836006ead456c936e97e64d2d4)

06-07 05:18:44.375 29762 29762 F DEBUG : #17 pc 000000000012de8 /system/lib64/libutils.so (thread_data_t::trampoline(thread_data_t const*)+408) (BuildId:

b940f836006ead456c936e97e64d2d4)

06-07 05:18:44.375 29762 29762 F DEBUG : #18 pc 0000000000b6a24 /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+264) (BuildId:

369edc656806aeaf384cbeb8f7a347af)

06-07 05:18:44.375 29762 29762 F DEBUG : #19 pc 00000000000532bc /apex/com.android.runtime/lib64/bionic/libc.so (_start_thread+68) (BuildId:

369edc656806aeaf384cbeb8f7a347af)

#3 - 2023-06-07 15:33 - CD TEST-方永红

- Status changed from RESOLVED to VERIFIED

#4 - 2023-06-07 15:33 - CD TEST-方永红

- Status changed from VERIFIED to CLOSED