PUBG MOBILE - OperationQueueImp crash with ANGLE

+1 5 Hotlists (4) Mark as Duplicate

Comments (17) Dependencies Duplicates (1) Blocking (0) Resources (5)

Obsolete Bug P1 + Add Hotlist

STATUS UPDATE No update yet. Edit

DESCRIPTION ia...@google.com created issue #1

After fixing another crash (debug-util marker related), I did a little game play after getting an AGI frame capture. The game played for a short time, froze and crashed on Pixel 4. I had just updated

I captured the AGI frame capture shortly after landing (from parachute), and the crash occured as I was running, shortly after taking the trace.

I tried reproducing the crash when not using AGI, and the game played fine.

Here's some relevant logcat:

```
06-18 17:04:33.795 23580 23628 I ANGLE   : Version (2.1.15987 git hash: 3706f9ebb517), Renderer (Vulkan 1.1.128 (Adreno (TM) 640 (0x06040001)))
...
06-18 17:10:24.637 23580 23878 I ANGLE   : EVENT: glDrawElements(context = 6, mode = GL_TRIANGLES, count = 4542, type = GL_UNSIGNED_SHORT, indices = 0x000000
06-18 17:10:24.760 23580 26844 I GCloudVoice: [/Users/apollo/GVoice/GCloudVoice/build/Android/jni/../../..//cdnvister/build/Android/jni/../../../src/room_age
--------- beginning of crash
06-18 17:10:24.834 23580 23878 F libc    : Fatal signal 11 (SIGSEGV), code -6 (SI_TKILL) in tid 23878 (RenderThread 1), pid 23580 (MainThread-UE4)
06-18 17:10:25.041 27498 27498 I crash_dump64: obtaining output fd from tombstoned, type: kDebuggerdTombstone
06-18 17:10:25.036 23580 23580 W Thread-290: type=1400 audit(0.0:4377): avc: denied { search } for name="thermal" dev="sysfs" ino=49344 scontext=u:r:untruste
06-18 17:10:25.043   969   969 I tombstoned: received crash request for pid 23878
06-18 17:10:25.044 27498 27498 I crash_dump64: performing dump of process 23580 (target tid = 23878)
06-18 17:10:25.055 27498 27498 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
06-18 17:10:25.055 27498 27498 F DEBUG   : Build fingerprint: 'google/flame/flame:11/RQ2A.210305.006/7119741:userdebug/dev-keys'
06-18 17:10:25.055 27498 27498 F DEBUG   : Revision: 'DVT1.0'
06-18 17:10:25.055 27498 27498 F DEBUG   : ABI: 'arm64'
06-18 17:10:25.058 27498 27498 F DEBUG   : Timestamp: 2021-06-18 17:10:25-0600
06-18 17:10:25.058 27498 27498 F DEBUG   : pid: 23580, tid: 23878, name: RenderThread 1  >>> com.tencent.ig <<<
06-18 17:10:25.058 27498 27498 F DEBUG   : uid: 10318
06-18 17:10:25.058 27498 27498 F DEBUG   : signal 11 (SIGSEGV), code -6 (SI_TKILL), fault addr --------
06-18 17:10:25.058 27498 27498 F DEBUG   : Abort message: '[2021-06-18 17:04:24 591] | Event | [GCloud] |0x77839b34f8| OperationQueueImp.cpp:112|OperationQue
06-18 17:10:25.058 27498 27498 F DEBUG   :     x0  00000074739df1e8  x1  0000000000000000  x2  0000000000000001  x3  000000747bcf6698
06-18 17:10:25.058 27498 27498 F DEBUG   :     x4  000000747bcf6a70  x5  0000000000000000  x6  000000747bcf6a58  x7  000000747bcf6a6c
06-18 17:10:25.058 27498 27498 F DEBUG   :     x8  0000000000000001  x9  00000074739df0c0  x10 0000007473e34ba4  x11 0000000000000040
06-18 17:10:25.058 27498 27498 F DEBUG   :     x12 00000000000000a0  x13 0000000000000008  x14 0000007473d379f4  x15 0000000000000007
06-18 17:10:25.058 27498 27498 F DEBUG   :     x16 00000074740bb2f8  x17 000000777f6cbce0  x18 0000000000000000  x19 00000076ed13c0c0
06-18 17:10:25.058 27498 27498 F DEBUG   :     x20 0000000000000090  x21 00000076ed13c9e8  x22 0000000000000001  x23 00000007fdc6a700
06-18 17:10:25.058 27498 27498 F DEBUG   :     x24 000000747bcf8000  x25 000000747473980d47  x26 00000074739afca7  x27 00000074739b9aae
06-18 17:10:25.058 27498 27498 F DEBUG   :     x28 000000747bcf8000  x29 000000747bcf6bc8
06-18 17:10:25.058 27498 27498 F DEBUG   :     lr  0000007473e34a74  sp  000000747bcf6a60  pc  0000007473e34db0  pst 0000000080000000
06-18 17:10:25.133 27498 27498 F DEBUG   : backtrace:
06-18 17:10:25.134 27498 27498 F DEBUG   :       #00 pc 0000000000601db0  /data/app/~~1UQn9XIabssKPi93AjlU-w==/org.chromium.angle-G9qnnPmd2iDv3gj2qi2r_w==/ba
06-18 17:10:25.134 27498 27498 F DEBUG   :       #01 pc 00000000006080b0  /data/app/~~1UQn9XIabssKPi93AjlU-w==/org.chromium.angle-G9qnnPmd2iDv3gj2qi2r_w==/ba
06-18 17:10:25.134 27498 27498 F DEBUG   :       #02 pc 00000000006087dc  /data/app/~~1UQn9XIabssKPi93AjlU-w==/org.chromium.angle-G9qnnPmd2iDv3gj2qi2r_w==/ba
06-18 17:10:25.134 27498 27498 F DEBUG   :       #03 pc 000000000060e664  /data/app/~~1UQn9XIabssKPi93AjlU-w==/org.chromium.angle-G9qnnPmd2iDv3gj2qi2r_w==/ba
06-18 17:10:25.134 27498 27498 F DEBUG   :       #04 pc 00000000002e6d78  /data/app/~~1UQn9XIabssKPi93AjlU-w==/org.chromium.angle-G9qnnPmd2iDv3gj2qi2r_w==/ba
06-18 17:10:25.134 27498 27498 F DEBUG   :       #05 pc 0000000004099828  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #06 pc 00000000041daa48  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #07 pc 000000000432b908  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.036 23580 23580 W Thread-290: type=1400 audit(0.0:4378): avc: denied { search } for name="thermal" dev="sysfs" ino=49344 scontext=u:r:untruste
06-18 17:10:25.134 27498 27498 F DEBUG   :       #08 pc 000000000432a8d4  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #09 pc 00000000043229ac  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:23.893   592   592 D logd    : logdr: UID=10318 GID=10318 PID=27494 n tail=1000 logMask=99 pid=0 start=0ns timeout=0ns
06-18 17:10:25.134 27498 27498 F DEBUG   :       #10 pc 000000000435f46c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #11 pc 0000000004407880  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #12 pc 000000000440b2ec  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #13 pc 0000000003804a50  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #14 pc 0000000003804694  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #15 pc 0000000003cde5b0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #16 pc 0000000003ce5de0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #17 pc 000000000383c9fc  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #18 pc 0000000003802c44  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib/ar
06-18 17:10:25.134 27498 27498 F DEBUG   :       #19 pc 00000000000afd4c  /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+64) (BuildId
06-18 17:10:25.134 27498 27498 F DEBUG   :       #20 pc 0000000000050288  /apex/com.android.runtime/lib64/bionic/libc.so (__start_thread+64) (BuildId: 49090a
```

✓ Links (5)

Links (5)

“https://source.android.com/devices/tech/debug/gdb”
“In Diagnosing Native Crashes the "TI_KILL" is associated with an abort.”
“ …erationQueueImp.cpp, and looking at the few results (and Image results), they all seem associated with PUGB or another tencent game. Best example is: Mi 9T pubg crash .”
“For completeness, here's the stack trace I got yesterday. This was doing game play after I took the AGI frame capture, this time with AGI not removing Vulkan extensions it didn't know about. The
“The Pixel 6 and 7 families of phones (that have Android 13 or greater) have ANGLE installed. The instructions in this doc show how to use ANGLE for a given game (the "per-application switch").”

COMMENTS

ia...@google.com <ia...@google.com> #2

I tried bisecting. Here's what I'm finding:

- ANGLE tag revision date Chromium revision

- BAD: 4546+ 3706f9ebb 6/18 368dacd8dc53
- Bad: 4534 1b680b772 6/4 fed1a144db8a diff stack1
- Bad: 4529 96ab65664 5/31 b65770476af8 diff stack2
- Note: 4526 - 4529 is just auto-rolls
- Bad: b6bd039cc 5/28 ed36a7408427
- BAD: 5e631c5ff keep keep
- Good: 05baaa37a keep keep
- Good: 4525 2622c7b04 5/27 b6af002ef64a
- Good: 4522 91e693afc 5/24 7bfc870f82dd

The stack trace for the 1b680b772 revision is similar but different than above:

```
06-21 14:39:11.465 27380 27380 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
06-21 14:39:11.465 27380 27380 F DEBUG   : Build fingerprint: 'google/flame/flame:11/RQ2A.210305.006/7119741:userdebug/dev-keys'
06-21 14:39:11.465 27380 27380 F DEBUG   : Revision: 'DVT1.0'
06-21 14:39:11.465 27380 27380 F DEBUG   : ABI: 'arm64'
06-21 14:39:11.467 27380 27380 F DEBUG   : Timestamp: 2021-06-21 14:39:11-0600
06-21 14:39:11.467 27380 27380 F DEBUG   : pid: 23238, tid: 23614, name: RenderThread 1  >>> com.tencent.ig <<<
06-21 14:39:11.467 27380 27380 F DEBUG   : uid: 10318
06-21 14:39:11.467 27380 27380 F DEBUG   : signal 11 (SIGSEGV), code -6 (SI_TKILL), fault addr --------
06-21 14:39:11.467 27380 27380 F DEBUG   : Abort message: '[2021-06-21 14:32:26 839] | Event | [GCloud] |0x77839b34f8| OperationQueueImp.cpp:112|Operation
06-21 14:39:11.467 27380 27380 F DEBUG   :     x0  00000007fd52afc0  x1  00000075bd87ebd0  x2  0000000000000110  x3  00000007fd52afc0
06-21 14:39:11.467 27380 27380 F DEBUG   :     x4  00000075bd87ed30  x5  00000007fd52b160  x6  403b87844039c6b8  x7  0000000040533333
06-21 14:39:11.467 27380 27380 F DEBUG   :     x8  4434000044be0000  x9  3ab60b613a2c7692  x10 37916126bf800000  x11 00000000389fde30
06-21 14:39:11.468 27380 27380 F DEBUG   :     x12 3d5f9df83d2ec1be  x13 3e6f8bb73dce0702  x14 ff00000000000000  x15 ffffffffffffffff
06-21 14:39:11.468 27380 27380 F DEBUG   :     x16 00000074725355e8  x17 000000777f6652c0  x18 0000000000000000  x19 0000000000000001
06-21 14:39:11.468 27380 27380 F DEBUG   :     x20 00000076cd713a70  x21 00000076cd713ad0  x22 0000007431402448  x23 00000076cd7139b0
06-21 14:39:11.468 27380 27380 F DEBUG   :     x24 0000000000000004  x25 00000076cd713df0  x26 0000007471dd4f8e  x27 0000007471e2ed90
06-21 14:39:09.925 23256 23256 I binder  : 23238:23256 ioctl c0306201 7488140a10 returned -4
06-21 14:39:11.468 27380 27380 F DEBUG   :     x28 00000007fd52ae40  x29 0000007431402560
06-21 14:39:11.468 27380 27380 F DEBUG   :     lr  00000074722faed0  sp  0000007431402360  pc  000000777f665278  pst 0000000020000000
06-21 14:39:09.926 23257 23257 I binder  : 23238:23257 ioctl c0306201 7487042a10 returned -4
06-21 14:39:11.545 27380 27380 F DEBUG   : backtrace:
06-21 14:39:11.545 27380 27380 F DEBUG   :       #00 pc 000000000004a278  /apex/com.android.runtime/lib64/bionic/libc.so (__memcpy+296) (BuildId: 49090ae5
06-21 14:39:11.569 23238 23238 W Thread-325: type=1400 audit(0.0:6393): avc: denied { search } for name="thermal" dev="sysfs" ino=49344 scontext=u:r:untru
06-21 14:39:11.545 27380 27380 F DEBUG   :       #01 pc 000000000062becc  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 14:39:11.545 27380 27380 F DEBUG   :       #02 pc 00000000005f4a10  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 14:39:11.545 27380 27380 F DEBUG   :       #03 pc 00000000005f52cc  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 14:39:11.545 27380 27380 F DEBUG   :       #04 pc 00000000005fb83c  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 14:39:11.545 27380 27380 F DEBUG   :       #05 pc 00000000003ab030  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 14:39:11.545 27380 27380 F DEBUG   :       #06 pc 00000000002eb3d8  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 14:39:11.545 27380 27380 F DEBUG   :       #07 pc 000000000409981c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #08 pc 00000000041daa48  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #09 pc 0000000004334e60  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #10 pc 000000000433362c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #11 pc 0000000004336170  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #12 pc 00000000043325c4  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #13 pc 000000000432342c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #14 pc 00000000043225c8  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #15 pc 000000000435f46c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #16 pc 0000000004407880  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #17 pc 000000000440b2ec  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #18 pc 0000000003804a50  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #19 pc 0000000003804694  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #20 pc 00000000003cde5b0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #21 pc 00000000003ce5de0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #22 pc 000000000383c9fc  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 14:39:11.545 27380 27380 F DEBUG   :       #23 pc 0000000003802c44  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
```

```
06-21 14:39:11.545 27380 27380 F DEBUG   :       #24 pc 00000000000afd4c  /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+64) (Buil
06-21 14:39:11.545 27380 27380 F DEBUG   :       #25 pc 0000000000050288  /apex/com.android.runtime/lib64/bionic/libc.so (__start_thread+64) (BuildId: 490
```

Diff stack2: The crash with commit 96ab65664 is very different:

```
06-21 15:05:48.349 30605 30605 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
06-21 15:05:48.349 30605 30605 F DEBUG   : Build fingerprint: 'google/flame/flame:11/RQ2A.210305.006/7119741:userdebug/dev-keys'
06-21 15:05:48.349 30605 30605 F DEBUG   : Revision: 'DVT1.0'
06-21 15:05:48.349 30605 30605 F DEBUG   : ABI: 'arm64'
06-21 15:05:48.352 30605 30605 F DEBUG   : Timestamp: 2021-06-21 15:05:48-0600
06-21 15:05:48.352 30605 30605 F DEBUG   : pid: 28193, tid: 28489, name: RenderThread 1  >>> com.tencent.ig <<<
06-21 15:05:48.352 30605 30605 F DEBUG   : uid: 10318
06-21 15:05:48.352 30605 30605 F DEBUG   : signal 11 (SIGSEGV), code -6 (SI_TKILL), fault addr --------
06-21 15:05:48.352 30605 30605 F DEBUG   : Abort message: '[2021-06-21 15:00:04 010] | Event | [GCloud] |0x77839b34f8| OperationQueueImp.cpp:112|Operation
06-21 15:05:48.352 30605 30605 F DEBUG   :     x0  00000007f56c6864  x1  000000745cad5630  x2  0000000000000000  x3  000000747e4c9260
06-21 15:05:48.352 30605 30605 F DEBUG   :     x4  000000745cad563c  x5  00000007f56c6870  x6  0000000300010000  x7  0002000300000003
06-21 15:05:48.352 30605 30605 F DEBUG   :     x8  000000755dd3a360  x9  e9a7d7e674f091fd  x10 0000000000000002  x11 0000000000000000
06-21 15:05:48.352 30605 30605 F DEBUG   :     x12 0000000000000000  x13 0000000000002210  x14 0033d43eff579b8d  x15 0000000003eea08e
06-21 15:05:48.352 30605 30605 F DEBUG   :     x16 00000074751af5e8  x17 000000777f6652c0  x18 0000000000000000  x19 000000745cad5630
06-21 15:05:48.352 30605 30605 F DEBUG   :     x20 00000076ed0fc080  x21 0000000000000006  x22 0000000000000001  x23 00000075fd0b96f0
06-21 15:05:48.352 30605 30605 F DEBUG   :     x24 00000075fd0b9988  x25 000000000000000c  x26 000000747e4cc000  x27 000000747e4c9938
06-21 15:05:48.352 30605 30605 F DEBUG   :     x28 000000747e4cc000  x29 000000747e4c9530
06-21 15:05:48.352 30605 30605 F DEBUG   :     lr  0000007474fad0ec  sp  000000747e4c9400  pc  000000777f6651b0  pst 0000000020000000
06-21 15:05:48.376 30605 30605 F DEBUG   : backtrace:
06-21 15:05:48.376 30605 30605 F DEBUG   :     NOTE: Function names and BuildId information is missing for some frames due
06-21 15:05:48.376 30605 30605 F DEBUG   :     NOTE: to unreadable libraries. For unwinds of apps, only shared libraries
06-21 15:05:48.376 30605 30605 F DEBUG   :     NOTE: found under the lib/ directory are readable.
06-21 15:05:48.376 30605 30605 F DEBUG   :     NOTE: On this device, run setenforce 0 to make the libraries readable.
06-21 15:05:48.376 30605 30605 F DEBUG   :       #00 pc 000000000004a1b0  /apex/com.android.runtime/lib64/bionic/libc.so (__memcpy+96) (BuildId: 49090ae59
06-21 15:05:48.376 30605 30605 F DEBUG   :       #01 pc 00000000006640e8  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 15:05:48.376 30605 30605 F DEBUG   :       #02 pc 00000000005f528c  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 15:05:48.376 30605 30605 F DEBUG   :       #03 pc 00000000005fb03c  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 15:05:48.376 30605 30605 F DEBUG   :       #04 pc 00000000002ddb58  /data/app/~~sJmFp4f8GpsSeRGvKd5n7g==/org.chromium.angle-2IlFCgawzX9ygOgiJooUBw==
06-21 15:05:48.376 30605 30605 F DEBUG   :       #05 pc 000000000409ace4  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #06 pc 00000000041167d0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #07 pc 0000000004cf2dd0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:49.664  1007  1007 W healthd : battery l=100 v=4379 t=38.5 h=2 st=5 c=1562 fc=2765000 cc=6 chg=a
06-21 15:05:48.376 30605 30605 F DEBUG   :       #08 pc 00000000053ed78c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #09 pc 00000000053ed924  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #10 pc 0000000003804a50  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:50.129 28193 28193 W Timer-1 : type=1400 audit(0.0:7051): avc: denied { search } for name="thermal" dev="sysfs" ino=49344 scontext=u:r:untrust
06-21 15:05:48.376 30605 30605 F DEBUG   :       #11 pc 0000000003804694  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #12 pc 0000000003cde5b0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #13 pc 0000000003ce5de0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #14 pc 000000000383c9fc  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #15 pc 0000000003802c44  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 15:05:48.376 30605 30605 F DEBUG   :       #16 pc 00000000000afd4c  /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+64) (Buil
06-21 15:05:48.376 30605 30605 F DEBUG   :       #17 pc 0000000000050288  /apex/com.android.runtime/lib64/bionic/libc.so (__start_thread+64) (BuildId: 490
```

ia...@google.com <ia...@google.com> #3

Reassigned to cc...@google.com.

I narrowed this down to the following commit:

```
5e631c5ff (HEAD) Vulkan: Disable shadowBuffers feature
```

The most-recent crash logcat looks like:

```
06-21 16:36:58.673 16565 16854 I ANGLE   : EVENT: glDrawElements(context = 6, mode = GL_TRIANGLES, count = 52380, type = GL_UNSIGNED_INT, indices = 0x000C
06-21 16:36:57.363 15881 15881 I google_charger: usbchg=USB_CDP typec=C usbv=4944 usbc=822 usbMv=5000 usbMc=1500
06-21 16:36:57.364 15881 15881 I sm8150_bms: MSC_PCS chg_state=5dc111f04030009 [0x9:4:3:4383:1500] chg=u
06-21 16:36:57.364 15881 15881 I google_battery: MSC_DIN chg_state=5dc111f04030009 f=0x9 chg_s=Not Charging chg_t=Taper vchg=4383 icl=1500
06-21 16:36:57.366 15881 15881 I google_battery: MSC_DSG vbatt_idx:2->2 vbatt=4377343 ibatt=937 fv_uv=4400000 cv_cnt=0 ov_cnt=0
06-21 16:36:57.367 15881 15881 I google_battery: MSC_LOGIC cv_cnt=0 ov_cnt=0 temp_idx:2->2, vbatt_idx:2->2, fv=4400000->4400000, cc_max=0
06-21 16:36:57.367 15881 15881 I google_battery: MSC_VOTE fv_uv=4400000 cc_max=0 update_interval=-1
06-21 16:36:57.367 15881 15881 I google_charger: MSC_CHG fv_uv=4400000, cc_max=0, rerun in 2000 ms (0)
--------- beginning of crash
06-21 16:36:58.827 16565 16854 F libc    : Fatal signal 11 (SIGSEGV), code -6 (SI_TKILL) in tid 16854 (RenderThread 1), pid 16565 (MainThread-UE4)
06-21 16:36:58.873   996 13156 D qc_adm  : ns 1627212 > expected_ns 1000000 (skipped 11743)
06-21 16:36:58.877   996 13156 D qc_adm  : ns 1577524 > expected_ns 1000000 (skipped 11743)
06-21 16:36:58.881   996 13156 D qc_adm  : ns 1639607 > expected_ns 1000000 (skipped 11743)
06-21 16:36:58.885   996 13156 D qc_adm  : ns 1680128 > expected_ns 1000000 (skipped 11743)
06-21 16:36:58.895   996 13156 D qc_adm  : ns 1526481 > expected_ns 1000000 (skipped 11743)
06-21 16:36:58.917   996 13156 D qc_adm  : ns 1646062 > expected_ns 1000000 (skipped 11743)
06-21 16:36:58.921   996 13156 D qc_adm  : ns 1604447 > expected_ns 1000000 (skipped 11743)
06-21 16:36:57.517 16583 16583 I binder  : 16565:16583 ioctl c0306201 7489140a10 returned -4
06-21 16:36:57.517 16585 16585 I binder  : 16565:16585 ioctl c0306201 7488042a10 returned -4
06-21 16:36:57.517 16586 16586 I binder  : 16565:16586 ioctl c0306201 7485f44a10 returned -4
06-21 16:36:57.520 16723 16723 I binder  : 16565:16723 ioctl c0306201 7438319a10 returned -4
```

```
06-21 16:36:57.520 16732 16732 I binder  : 16565:16732 ioctl c0306201 74dead7a10 returned -4
06-21 16:36:57.521 16799 16799 I binder  : 16565:16799 ioctl c0306201 741869da10 returned -4
06-21 16:36:57.522 16837 16837 I binder  : 16565:16837 ioctl c0306201 744e35da10 returned -4
06-21 16:36:59.011   996 13156 D qc_adm  : ns 1678397 > expected_ns 1000000 (skipped 11743)
06-21 16:36:57.559   592   592 D logd    : logdr: UID=10318 GID=10318 PID=20842 n tail=1000 logMask=99 pid=0 start=0ns timeout=0ns
06-21 16:36:59.034 20843 20843 I crash_dump64: obtaining output fd from tombstoned, type: kDebuggerdTombstone
06-21 16:36:57.946   592   592 D logd    : logdr: UID=10318 GID=10318 PID=20843 n tail=50 logMask=8 pid=16565 start=0ns timeout=0ns
06-21 16:36:58.630   285   285 I msm-dsi-display: [dsi_display_force_update_dsi_clk] dsi bit clk has been configured to 0
06-21 16:36:58.714   592   592 D logd    : logdr: UID=10318 GID=10318 PID=20849 n tail=0 logMask=99 pid=0 start=0ns timeout=0ns
06-21 16:36:59.371 15881 15881 I google_charger: usbchg=USB_CDP typec=C usbv=5048 usbc=576 usbMv=5000 usbMc=1500
06-21 16:36:59.371 15881 15881 I sm8150_bms: MSC_PCS chg_state=5dc111f04030009 [0x9:4:3:4383:1500] chg=u
06-21 16:36:59.371 15881 15881 I google_battery: MSC_DIN chg_state=5dc111f04030009 f=0x9 chg_s=Not Charging chg_t=Taper vchg=4383 icl=1500
06-21 16:36:59.374 15881 15881 I google_battery: MSC_DSG vbatt_idx:2->2 vbatt=4377343 ibatt=937 fv_uv=4400000 cv_cnt=0 ov_cnt=0
06-21 16:36:59.374 15881 15881 I google_battery: MSC_LOGIC cv_cnt=0 ov_cnt=0 temp_idx:2->2, vbatt_idx:2->2, fv=4400000->4400000, cc_max=0
06-21 16:36:59.035   996 13156 D qc_adm  : ns 1613863 > expected_ns 1000000 (skipped 11743)
06-21 16:36:59.036   969   969 I tombstoned: received crash request for pid 16854
06-21 16:36:59.030 16565 16565 W Thread-324: type=1400 audit(0.0:9670): avc: denied { search } for name="thermal" dev="sysfs" ino=49344 scontext=u:r:untru
06-21 16:36:59.037 20843 20843 I crash_dump64: performing dump of process 16565 (target tid = 16854)
06-21 16:36:59.374 15881 15881 I google_battery: MSC_VOTE fv_uv=4400000 cc_max=0 update_interval=-1
06-21 16:36:59.051 20843 20843 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
06-21 16:36:59.051 20843 20843 F DEBUG   : Build fingerprint: 'google/flame/flame:11/RQ2A.210305.006/7119741:userdebug/dev-keys'
06-21 16:36:59.051 20843 20843 F DEBUG   : Revision: 'DVT1.0'
06-21 16:36:59.051 20843 20843 F DEBUG   : ABI: 'arm64'
06-21 16:36:59.052 20843 20843 F DEBUG   : Timestamp: 2021-06-21 16:36:59-0600
06-21 16:36:59.052 20843 20843 F DEBUG   : pid: 16565, tid: 16854, name: RenderThread 1  >>> com.tencent.ig <<<
06-21 16:36:59.052 20843 20843 F DEBUG   : uid: 10318
06-21 16:36:59.052 20843 20843 F DEBUG   : signal 11 (SIGSEGV), code -6 (SI_TKILL), fault addr --------
06-21 16:36:59.052 20843 20843 F DEBUG   : Abort message: '[2021-06-21 16:31:25 245] | Event | [GCloud] |0x77839b34f8| OperationQueueImp.cpp:112|Operation
06-21 16:36:59.052 20843 20843 F DEBUG   :     x0  00000007fd89b000  x1  00000075ad2375d0  x2  0000000000000150  x3  00000007fd89b000
06-21 16:36:59.052 20843 20843 F DEBUG   :     x4  00000075ad237720  x5  00000007fd89b150  x6  b39a982f3f63ed43  x7  3f2a2bc700000000
06-21 16:36:59.052 20843 20843 F DEBUG   :     x8  0000000000000000  x9  0000000000000000  x10 e9a7d7e674f091fd  x11 0000000000000000
06-21 16:36:59.052 20843 20843 F DEBUG   :     x12 33898d9cbf4acd49  x13 3f3f40d900000000  x14 0027f0cde0647520  x15 00000000041ee072
06-21 16:36:59.052 20843 20843 F DEBUG   :     x16 0000007473d668d8  x17 000000777f6652c0  x18 0000000000000000  x19 0000000000000000
06-21 16:36:59.052 20843 20843 F DEBUG   :     x20 00000076cd4ff710  x21 00000076cd4ff830  x22 000000743074e8c8  x23 00000076cd4ff710
06-21 16:36:59.052 20843 20843 F DEBUG   :     x24 0000000000000000  x25 00000076cd4ffb50  x26 0000000747361382d  x27 000000747366cfdc
06-21 16:36:59.052 20843 20843 F DEBUG   :     x28 00000007fd89b000  x29 000000743074e9e0
06-21 16:36:59.052 20843 20843 F DEBUG   :     lr  0000007473b375fc  sp  000000743074e7e0  pc  000000777f665248  pst 0000000020000000
06-21 16:36:59.083   996 13156 D qc_adm  : ns 1644223 > expected_ns 1000000 (skipped 11743)
06-21 16:36:59.122 20843 20843 F DEBUG   : backtrace:
06-21 16:36:59.122 20843 20843 F DEBUG   :       #00 pc 000000000004a248  /apex/com.android.runtime/lib64/bionic/libc.so (__memcpy+248) (BuildId: 49090ae5
06-21 16:36:59.122 20843 20843 F DEBUG   :       #01 pc 00000000006295f8  /data/app/~~wEUe28gGCuTW3Hz7SrhAKg==/org.chromium.angle-mN6p2_3wxh0Pz45QEcpvTA==
06-21 16:36:59.123 20843 20843 F DEBUG   :       #02 pc 00000000005f2030  /data/app/~~wEUe28gGCuTW3Hz7SrhAKg==/org.chromium.angle-mN6p2_3wxh0Pz45QEcpvTA==
06-21 16:36:59.374 15881 15881 I google_charger: MSC_CHG fv_uv=4400000, cc_max=0, rerun in 2000 ms (0)
06-21 16:36:59.767   592   592 D logdd   : logdr: UID=10318 GID=10318 PID=20843 n tail=50 logMask=1 pid=16565 start=0ns timeout=0ns
06-21 16:37:01.379 15881 15881 I google_charger: usbchg=USB_CDP typec=C usbv=5067 usbc=387 usbMv=5000 usbMc=1500
06-21 16:36:59.123 20843 20843 F DEBUG   :       #03 pc 00000000005f28ec  /data/app/~~wEUe28gGCuTW3Hz7SrhAKg==/org.chromium.angle-mN6p2_3wxh0Pz45QEcpvTA==
06-21 16:36:59.030 16565 16565 W Thread-324: type=1400 audit(0.0:9671): avc: denied { search } for name="thermal" dev="sysfs" ino=49344 scontext=u:r:untru
06-21 16:36:59.123 20843 20843 F DEBUG   :       #04 pc 00000000005f8658  /data/app/~~wEUe28gGCuTW3Hz7SrhAKg==/org.chromium.angle-mN6p2_3wxh0Pz45QEcpvTA==
06-21 16:36:59.123 20843 20843 F DEBUG   :       #05 pc 00000000002db8b8  /data/app/~~wEUe28gGCuTW3Hz7SrhAKg==/org.chromium.angle-mN6p2_3wxh0Pz45QEcpvTA==
06-21 16:36:59.123 20843 20843 F DEBUG   :       #06 pc 0000000004099828  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #07 pc 00000000041daa48  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #08 pc 0000000004334c60  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #09 pc 00000000043360dc  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #10 pc 00000000043325c4  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #11 pc 0000000004322b64  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #12 pc 000000000435f46c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #13 pc 0000000004407880  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #14 pc 000000000440b2ec  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #15 pc 0000000003804a50  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #16 pc 0000000003804694  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #17 pc 0000000003cde5b0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #18 pc 0000000003ce5de0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #19 pc 000000000383c9fc  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #20 pc 0000000003802c44  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-21 16:36:59.123 20843 20843 F DEBUG   :       #21 pc 00000000000afd4c  /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+64) (Buil
06-21 16:36:59.123 20843 20843 F DEBUG   :       #22 pc 0000000000050288  /apex/com.android.runtime/lib64/bionic/libc.so (__start_thread+64) (BuildId: 490
```

ia...@google.com <ia...@google.com> #4

Want to try looking at what gdb can see. Charlie suggesting trying:

adb shell setprop debug.debuggerd.wait_for_debugger true

https://source.android.com/devices/tech/debug/gdb

ia...@google.com <ia...@google.com> #5

tl;dr: `OperationQueueImp` seems to be something in tencent games that is killing the game.

I did some searching about `OperationQueueImp.` I first tried ANGLE codesearch, and then Android codesearch. I then tried Google search and got a few hits.

1. In Diagnosing Native Crashes the "TI_KILL" is associated with an abort.
2. Searching for `OperationQueueImp.cpp`, and looking at the few results (and Image results), they all seem associated with PUGB or another tencent game. Best example is: Mi 9T put

If PUBG has something that is killing the game, that could definitely explain the random stack traces, as well as why they've only occured (for me) while doing an AGI frame capture (which slo

I decided to search for this because I noticed that Charlie's stack trace also had that in it, and he was crashing at startup for a known issue. Yet, he also got that same:

> Abort message: '[2021-06-22 14:18:52 191] | Event | [GCloud] |0x738d1b64f8| OperationQueueImp.cpp:112|OperationQueueImp| OperationQueueImp66(0x7175462f10)

All of my stack traces had the same `OperationQueueImp.cpp:112|OperationQueueImp| OperationQueueImp66` string in them, that starts off with `Abort message` and has `Event | [GC`

---

ia...@google.com <ia...@google.com> #6

For completeness, here's the stack trace I got yesterday. This was doing game play after I took the AGI frame capture, this time with AGI not removing Vulkan extensions it didn't know about.

```
06-22 18:41:09.243 20577 20577 F DEBUG   : Timestamp: 2021-06-22 18:41:09-0600
06-22 18:41:09.243 20577 20577 F DEBUG   : pid: 19132, tid: 19424, name: RenderThread 1  >>> com.tencent.ig <<<
06-22 18:41:09.243 20577 20577 F DEBUG   : uid: 10318
06-22 18:41:09.243 20577 20577 F DEBUG   : signal 11 (SIGSEGV), code -6 (SI_TKILL), fault addr --------
06-22 18:41:09.243 20577 20577 F DEBUG   : Abort message: '[2021-06-22 18:36:05 253] | Event | [GCloud] |0x77839b34f8| OperationQueueImp.cpp:112|Operation
06-22 18:41:09.243 20577 20577 F DEBUG   :     x0  00000075ad0a7b14  x1  0000000000000005  x2  0000000000000100  x3  000000747e5e1670
06-22 18:41:09.243 20577 20577 F DEBUG   :     x4  000000747e5e1820  x5  000000747e5e1818  x6  000000747e5e1810  x7  0000000000000000
06-22 18:41:09.243 20577 20577 F DEBUG   :     x8  00000007fd0a0900  x9  0000000000000014  x10 0000000000000014  x11 0000000000000000
06-22 18:41:09.243 20577 20577 F DEBUG   :     x12 0000000000000000  x13 0000000000000000  x14 00105f5eceb9cef2  x15 0000000004cd7792
06-22 18:41:09.243 20577 20577 F DEBUG   :     x16 00000074774507e8  x17 000000777f6cbce0  x18 0000000000000000  x19 0000000000000005
06-22 18:41:09.243 20577 20577 F DEBUG   :     x20 00000076ed16c0f0  x21 00000076ed16df20  x22 0000007476d280f4  x23 0000007476d4492c
06-22 18:41:09.243 20577 20577 F DEBUG   :     x24 000000747e5e3000  x25 0000007476d11ea0  x26 0000007476d4accc  x27 000000747e5e19e8
06-22 18:41:09.243 20577 20577 F DEBUG   :     x28 0000007476d3b32b  x29 000000747e5e1950
06-22 18:41:09.243 20577 20577 F DEBUG   :     lr  00000074771d0548  sp  000000747e5e1810  pc  00000074771d0550  pst 0000000020000000
06-22 18:41:10.554 19132 19132 W Timer-1 : type=1400 audit(0.0:15878): avc: denied { search } for name="thermal" dev="sysfs" ino=49344 scontext=u:r:untrus
06-22 18:41:09.313 19132 19205 V threaded_app: New input event: type=2
06-22 18:41:09.338 20577 20577 F DEBUG   : backtrace:
06-22 18:41:09.338 20577 20577 F DEBUG   :       #00 pc 000000000060c550  /data/app/~~4vQY6nXCFMJBaKJYJZwt5w==/org.chromium.angle-Q4LYonaFtWWmc8QgDTxJGg==
06-22 18:41:09.338 20577 20577 F DEBUG   :       #01 pc 0000000000600704  /data/app/~~4vQY6nXCFMJBaKJYJZwt5w==/org.chromium.angle-Q4LYonaFtWWmc8QgDTxJGg==
06-22 18:41:09.338 20577 20577 F DEBUG   :       #02 pc 0000000000608c90  /data/app/~~4vQY6nXCFMJBaKJYJZwt5w==/org.chromium.angle-Q4LYonaFtWWmc8QgDTxJGg==
06-22 18:41:09.338 20577 20577 F DEBUG   :       #03 pc 00000000006093bc  /data/app/~~4vQY6nXCFMJBaKJYJZwt5w==/org.chromium.angle-Q4LYonaFtWWmc8QgDTxJGg==
06-22 18:41:09.338 20577 20577 F DEBUG   :       #04 pc 000000000060fa44  /data/app/~~4vQY6nXCFMJBaKJYJZwt5w==/org.chromium.angle-Q4LYonaFtWWmc8QgDTxJGg==
06-22 18:41:09.338 20577 20577 F DEBUG   :       #05 pc 00000000003b47a4  /data/app/~~4vQY6nXCFMJBaKJYJZwt5w==/org.chromium.angle-Q4LYonaFtWWmc8QgDTxJGg==
06-22 18:41:09.338 20577 20577 F DEBUG   :       #06 pc 00000000002f4708  /data/app/~~4vQY6nXCFMJBaKJYJZwt5w==/org.chromium.angle-Q4LYonaFtWWmc8QgDTxJGg==
06-22 18:41:09.338 20577 20577 F DEBUG   :       #07 pc 000000000409981c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #08 pc 00000000041da9f4  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #09 pc 000000000432b908  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #10 pc 000000000432a8d4  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #11 pc 00000000043229ac  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #12 pc 000000000435f46c  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #13 pc 0000000004407880  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #14 pc 000000000440b2ec  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #15 pc 0000000003804a50  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #16 pc 0000000003804694  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #17 pc 0000000003cde5b0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #18 pc 0000000003ce5de0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #19 pc 000000000383c9fc  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #20 pc 0000000003802c44  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-22 18:41:09.338 20577 20577 F DEBUG   :       #21 pc 00000000000afd4c  /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+64) (Buil
06-22 18:41:09.338 20577 20577 F DEBUG   :       #22 pc 0000000000050288  /apex/com.android.runtime/lib64/bionic/libc.so (__start_thread+64) (BuildId: 490
```

---

ia...@google.com <ia...@google.com> #7

I speculated that the game was being killed because the frames were taking too long. I disabled the GN arg that caused ANGLE to log every GLES command. The game still crashed, but this t

```
06-23 17:32:07.822 14047 14047 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
06-23 17:32:07.822 14047 14047 F DEBUG   : Build fingerprint: 'google/flame/flame:11/RQ2A.210305.006/7119741:userdebug/dev-keys'
06-23 17:32:07.822 14047 14047 F DEBUG   : Revision: 'DVT1.0'
06-23 17:32:07.822 14047 14047 F DEBUG   : ABI: 'arm64'
06-23 17:32:07.823 14047 14047 F DEBUG   : Timestamp: 2021-06-23 17:32:07-0600
06-23 17:32:07.823 14047 14047 F DEBUG   : pid: 12465, tid: 12779, name: RenderThread 1  >>> com.tencent.ig <<<
06-23 17:32:07.823 14047 14047 F DEBUG   : uid: 10318
06-23 17:32:07.823 14047 14047 F DEBUG   : signal 11 (SIGSEGV), code -6 (SI_TKILL), fault addr --------
06-23 17:32:07.823 14047 14047 F DEBUG   : Abort message: '[2021-06-23 17:28:13 307] | Event | [GCloud] |0x75a8f0d4f8| OperationQueueImp.cpp:112|Operation
06-23 17:32:07.823 14047 14047 F DEBUG   :     x0  00000007fd207b00  x1  00000000000003ab  x2  00000075a4c4f27d  x3  0000007298eda796
06-23 17:32:07.823 14047 14047 F DEBUG   :     x4  0000000000000000  x5  0000000000000000  x6  0000000000000000  x7  0000000000000000
06-23 17:32:07.823 14047 14047 F DEBUG   :     x8  0000000000000001  x9  00000007fd207b18  x10 00000071d4e9b040  x11 000000003f4f6036
06-23 17:32:07.823 14047 14047 F DEBUG   :     x12 0000000000000000  x13 5f4c47207c205449  x14 00000075a580cd22  x15 0000000000000011
06-23 17:32:07.823 14047 14047 F DEBUG   :     x16 00000075a5297350  x17 00000075a57b0618  x18 00000000071fc64f  x19 000000723ad85040
06-23 17:32:07.823 14047 14047 F DEBUG   :     x20 00000071fc658e48  x21 0000000000000009  x22 00000071f7b2ba30  x23 0000000000000001
06-23 17:32:07.823 14047 14047 F DEBUG   :     x24 000000729829cd58  x25 00000071f7b2ba48  x26 0000000000000000  x27 00000000000001b0
```

```
06-23 17:32:07.823 14047 14047 F DEBUG   :     x28 0000000000000000  x29 00000072a3b729b0
06-23 17:32:07.823 14047 14047 F DEBUG   :     lr  00000072935bc3b4  sp  00000072a3b72930  pc  00000072935bc3d8  pst 0000000020000000
06-23 17:32:07.837 14047 14047 F DEBUG   : backtrace:
06-23 17:32:07.837 14047 14047 F DEBUG   :       #00 pc 0000000004ef23d8  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #01 pc 000000000528a224  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #02 pc 00000000052db6b4  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #03 pc 0000000003804a50  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #04 pc 0000000003804694  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #05 pc 0000000003cde5b0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #06 pc 0000000003ce5de0  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #07 pc 000000000383c9fc  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #08 pc 0000000003802c44  /data/app/~~VzDE8Ha2Bobb7yAzxph5Jg==/com.tencent.ig-ITQLVVx_GwDarBdoVDgKYg==/lib
06-23 17:32:07.837 14047 14047 F DEBUG   :       #09 pc 00000000000afd4c  /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+64) (Buil
06-23 17:32:07.837 14047 14047 F DEBUG   :       #10 pc 0000000000050288  /apex/com.android.runtime/lib64/bionic/libc.so (__start_thread+64) (BuildId: 490
```

cc...@google.com <cc...@google.com> #8

I have spend two days on this try to root cause it and still not able to. What I know so far is that this PBO is called glBufferData and then glMapBuffer and glUnmapBuffer. The difference betw
us one DMA copy, but this somehow breaks this specific app+AGI. If I enable mShadowBuffer so that application will write into shadow buffer, but mean time also go through code path whe
pointer to application. My current theory is that application is doing something bad, that it is holding onto the pointer returned from mapBuffer call and still accessing it after unmap() call.

For now to get AGI unblock, I suggest just enable mShadowBuffer on AGI release branch and I will keep digging on the exact root cause and fix.

ia...@google.com <ia...@google.com> #9

I just got this crash with the older, version 93.0.4522.0 official ANGLE APK, on a Pixel 4.

I played the game for a while before "livelock" killed PUBG. Then, I restarted the game and did a new match. The crash occured shortly after the airplane started.

That calls into question our thinking that this has to do with the shadow buffer

cc...@google.com <cc...@google.com> #10

Can we send this to developer to further investigation? I think there is an app bug involved and ANGLE just triggering this. Or at least there is no evidence indicating strongly it is angle bug.

ia...@google.com <ia...@google.com> #11

I will make this bug publicly visible so that Gerald Li can share with Tencent. We hope they can provide us with insight:

- Is the game killing itself?
- If so, why?
- Are there special requirements that PUBG has for the use of PBO and glBufferData, glMapBuffer, and glUnmapBuffer?

mi...@lunarg.com <mi...@lunarg.com> #12

I can reliably reproduce this issue on a Pixel 4. After capturing one or more frames with AGI, the application will die around 10-300 frames later.

It seems to be an interaction between the application and the AGI coherent memory tracker. If I disable coherent memory tracking the crash goes away. If I modify the memory tracker to "clea

My current thinking is that the application is replacing the SIGSEGV handler that AGI uses. If this happens while there are still write-protected pages, the next write to one of these pages will c
content to let the AGI handler exist for hundreds of frames until it starts tracking page writes, and then it is only a few frames more before I see it get replaced and then crash.

ia...@google.com <ia...@google.com> #13

Reassigned to ge...@google.com.

Thank you for your findings Mike. I am inclined to agree with Charlie that this could be an application bug; at least to the degree that it prevents AGI from being able to capture a trace.

I'm going to assign this to Gerald Li to see if Tencent has learned anything.

sy...@google.com <sy...@google.com> #14

Probably AGI could reassign the handler (and forward to the application's) if it detects changes.

ge...@google.com <ge...@google.com> #15

I have talk this several times with Tencent from last year. They also can not get any helpful info from the logs now.

There should be some Vulkan only device that run GLES on ANGLE, but they are not able to get the devices. Most issue of ANGLE are blocked by that they did not prioritize this as it not a iss

Do we have any update from our side now?

ia...@google.com <ia...@google.com> #16

The Exynos 2200 version of the Samsung Galaxy S22 family is Vulkan only with ANGLE being the GLES driver

The Exynos 2200 version of the Samsung Galaxy S22 family is Vulkan only with ANGLE being the GLES driver.
The Pixel 6 and 7 families of phones (that have Android 13 or greater) have ANGLE installed. The instructions in this doc show how to use ANGLE for a given game (the "per-application sw

sy...@google.com <sy...@google.com> #17

FWIW, Fuchsia devices are also Vulkan-only and run GLES on ANGLE.

lp...@google.com <lp...@google.com>

Status: Won't Fix (Obsolete)