Android Public Tracker   37013028

← C ☆ SIGSEGV in libunwind from surfaceflinger Android L Nexus 5   +1 2   Hotlists (1)   Mark as Duplicate   🔔   ⋮

Comments (7)   Dependencies   Duplicates (0)   Blocking (0)   Resources (1)

Obsolete   Bug   P4   + Add Hotlist

👥 STATUS UPDATE No update yet.   Edit

📄 DESCRIPTION [Deleted User] created issue #1

Ever since upgrading to 5.0 Lollipop on my Nexus 5, I have been experiencing totally random (however they seem more be prevalent whilst using Chrome Beta) crashes. I have posted several logs

If it helps, the screen tears vertically quite a bit when scrolling just before the crash occurs. When the crash does occur, the phone just promptly reboots on its own.

```
*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'google/hammerhead/hammerhead:5.0/LRX21O/1570415:user/release-keys'
Revision: '11'
ABI: 'arm'
pid: 26914, tid: 27301, name: Binder_3  >>> /system/bin/surfaceflinger <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x19
    r0 00000001  r1 00000000  r2 fffffff0  r3 b6e2cc60
    r4 00000001  r5 b241b140  r6 00000000  r7 b240d740
    r8 00000312  r9 b6f15df4  sl 00000018  fp 00000000
    ip b6e2cf58  sp b260da58  lr b6e2a7b5  pc b6d91386  cpsr 000f0030

backtrace:
    #00 pc 00002386  /system/lib/libunwind.so
    #01 pc 000047b1  /system/lib/libbacktrace.so (UnwindMap::~UnwindMap()+24)
    #02 pc 00004807  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+38)
    #03 pc 0000481d  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+4)
    #04 pc 0000493d  /system/lib/libbacktrace.so (BacktraceMap::Create(int, bool)+76)
    #05 pc 00003155  /system/lib/libbacktrace.so (Backtrace::Backtrace(BacktraceImpl*, int, BacktraceMap*)+52)
    #06 pc 0000317f  /system/lib/libbacktrace.so (BacktraceCurrent::BacktraceCurrent(BacktraceImpl*, BacktraceMap*)+22)
    #07 pc 0000405f  /system/lib/libbacktrace.so (CreateCurrentObj(BacktraceMap*)+28)
    #08 pc 0000cfe3  /system/lib/libutils.so (android::CallStack::update(int, int)+38)
    #09 pc 0000d107  /system/lib/libutils.so (android::CallStack::CallStack(char const*, int)+38)
    #10 pc 00023513  /system/lib/libbinder.so (android::Parcel::read(android::Parcel::FlattenableHelperInterface&) const+246)
    #11 pc 00033035  /system/lib/libgui.so (android::BnGraphicBufferProducer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+568)
    #12 pc 0001a6d9  /system/lib/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+60)
    #13 pc 0001f787  /system/lib/libbinder.so (android::IPCThreadState::executeCommand(int)+582)
    #14 pc 0001f8ab  /system/lib/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+38)
    #15 pc 0001f8ed  /system/lib/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+48)
    #16 pc 00023a5b  /system/lib/libbinder.so
    #17 pc 000104d5  /system/lib/libutils.so (android::Thread::_threadLoop(void*)+112)
    #18 pc 00010045  /system/lib/libutils.so
    #19 pc 000162e3  /system/lib/libc.so (__pthread_start(void*)+30)
    #20 pc 000142d3  /system/lib/libc.so (__start_thread+6)

*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'google/hammerhead/hammerhead:5.0/LRX21O/1570415:user/release-keys'
Revision: '11'
ABI: 'arm'
pid: 11249, tid: 15502, name: Binder_5  >>> /system/bin/surfaceflinger <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x15
    r0 fffffffd  r1 00000000  r2 fffffff0  r3 b6e13c60
    r4 fffffffd  r5 b1d1a040  r6 00000000  r7 b1d12150
    r8 00000166  r9 b6efcdf4  sl 00000018  fp 00000000
    ip b6e13f58  sp b21d2a58  lr b6e117b5  pc b6d78386  cpsr 000f0030

backtrace:
    #00 pc 00002386  /system/lib/libunwind.so
    #01 pc 000047b1  /system/lib/libbacktrace.so (UnwindMap::~UnwindMap()+24)
    #02 pc 00004807  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+38)
    #03 pc 0000481d  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+4)
    #04 pc 0000493d  /system/lib/libbacktrace.so (BacktraceMap::Create(int, bool)+76)
    #05 pc 00003155  /system/lib/libbacktrace.so (Backtrace::Backtrace(BacktraceImpl*, int, BacktraceMap*)+52)
    #06 pc 0000317f  /system/lib/libbacktrace.so (BacktraceCurrent::BacktraceCurrent(BacktraceImpl*, BacktraceMap*)+22)
    #07 pc 0000405f  /system/lib/libbacktrace.so (CreateCurrentObj(BacktraceMap*)+28)
    #08 pc 0000cfe3  /system/lib/libutils.so (android::CallStack::update(int, int)+38)
    #09 pc 0000d107  /system/lib/libutils.so (android::CallStack::CallStack(char const*, int)+38)
    #10 pc 00023513  /system/lib/libbinder.so (android::Parcel::read(android::Parcel::FlattenableHelperInterface&) const+246)
    #11 pc 00033035  /system/lib/libgui.so (android::BnGraphicBufferProducer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+568)
    #12 pc 0001a6d9  /system/lib/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+60)
    #13 pc 0001f787  /system/lib/libbinder.so (android::IPCThreadState::executeCommand(int)+582)
    #14 pc 0001f8ab  /system/lib/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+38)
    #15 pc 0001f8ed  /system/lib/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+48)
    #16 pc 00023a5b  /system/lib/libbinder.so
    #17 pc 000104d5  /system/lib/libutils.so (android::Thread::_threadLoop(void*)+112)
    #18 pc 00010045  /system/lib/libutils.so
```

```
    #19 pc 000162e3  /system/lib/libc.so (__pthread_start(void*)+30)
    #20 pc 000142d3  /system/lib/libc.so (__start_thread+6)


*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'google/hammerhead/hammerhead:5.0/LRX21O/1570415:user/release-keys'
Revision: '11'
ABI: 'arm'
pid: 23447, tid: 24639, name: Binder_4  >>> /system/bin/surfaceflinger <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x6c69748d
    r0 6c697475  r1 00000000  r2 fffffff0  r3 b6ea1c60
    r4 6c697475  r5 ad929100  r6 00000000  r7 ad90d380
    r8 0000018d  r9 b6f8adf4  sl 00000018  fp 00000000
    ip b6ea1f58  sp b16ffa58  lr b6e9f7b5  pc b6e06386  cpsr 000f0030


backtrace:
    #00 pc 00002386  /system/lib/libunwind.so
    #01 pc 000047b1  /system/lib/libbacktrace.so (UnwindMap::~UnwindMap()+24)
    #02 pc 00004807  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+38)
    #03 pc 0000481d  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+4)
    #04 pc 0000493d  /system/lib/libbacktrace.so (BacktraceMap::Create(int, bool)+76)
    #05 pc 00003155  /system/lib/libbacktrace.so (Backtrace::Backtrace(BacktraceImpl*, int, BacktraceMap*)+52)
    #06 pc 0000317f  /system/lib/libbacktrace.so (BacktraceCurrent::BacktraceCurrent(BacktraceImpl*, BacktraceMap*)+22)
    #07 pc 0000405f  /system/lib/libbacktrace.so (CreateCurrentObj(BacktraceMap*)+28)
    #08 pc 0000cfe3  /system/lib/libutils.so (android::CallStack::update(int, int)+38)
    #09 pc 0000d107  /system/lib/libutils.so (android::CallStack::CallStack(char const*, int)+38)
    #10 pc 00023513  /system/lib/libbinder.so (android::Parcel::read(android::Parcel::FlattenableHelperInterface&) const+246)
    #11 pc 00033035  /system/lib/libgui.so (android::BnGraphicBufferProducer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+568)
    #12 pc 0001a6d9  /system/lib/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+60)
    #13 pc 0001f787  /system/lib/libbinder.so (android::IPCThreadState::executeCommand(int)+582)
    #14 pc 0001f8ab  /system/lib/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+38)
    #15 pc 0001f8ed  /system/lib/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+48)
    #16 pc 00023a5b  /system/lib/libbinder.so
    #17 pc 000104d5  /system/lib/libutils.so (android::Thread::_threadLoop(void*)+112)
    #18 pc 00010045  /system/lib/libutils.so
    #19 pc 000162e3  /system/lib/libc.so (__pthread_start(void*)+30)
    #20 pc 000142d3  /system/lib/libc.so (__start_thread+6)


*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'google/hammerhead/hammerhead:5.0/LRX21O/1570415:user/release-keys'
Revision: '11'
ABI: 'arm'
pid: 12429, tid: 13394, name: Binder_4  >>> /system/bin/surfaceflinger <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x14
    r0 ffffffff  r1 fffffff4  r2 00000001  r3 b6f22fac
    r4 00000000  r5 fffffff28  r6 00000001  r7 b6f16650
    r8 000003e7  r9 0000000c  sl 00000018  fp 00000000
    ip b6da0f54  sp b21ff9f8  lr b6ec07a9  pc b6ef6bf8  cpsr 200f0030


backtrace:
    #00 pc 00048bf8  /system/lib/libc.so (ifree+47)
    #01 pc 000127a7  /system/lib/libc.so (free+10)
    #02 pc 0000239b  /system/lib/libunwind.so
    #03 pc 000047b1  /system/lib/libbacktrace.so (UnwindMap::~UnwindMap()+24)
    #04 pc 00004807  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+38)
    #05 pc 0000481d  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+4)
    #06 pc 0000493d  /system/lib/libbacktrace.so (BacktraceMap::Create(int, bool)+76)
    #07 pc 00003155  /system/lib/libbacktrace.so (Backtrace::Backtrace(BacktraceImpl*, int, BacktraceMap*)+52)
    #08 pc 0000317f  /system/lib/libbacktrace.so (BacktraceCurrent::BacktraceCurrent(BacktraceImpl*, BacktraceMap*)+22)
    #09 pc 0000405f  /system/lib/libbacktrace.so (CreateCurrentObj(BacktraceMap*)+28)
    #10 pc 0000cfe3  /system/lib/libutils.so (android::CallStack::update(int, int)+38)
    #11 pc 0000d107  /system/lib/libutils.so (android::CallStack::CallStack(char const*, int)+38)
    #12 pc 00023513  /system/lib/libbinder.so (android::Parcel::read(android::Parcel::FlattenableHelperInterface&) const+246)
    #13 pc 00033035  /system/lib/libgui.so (android::BnGraphicBufferProducer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+568)
    #14 pc 0001a6d9  /system/lib/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+60)
    #15 pc 0001f787  /system/lib/libbinder.so (android::IPCThreadState::executeCommand(int)+582)
    #16 pc 0001f8ab  /system/lib/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+38)
    #17 pc 0001f8ed  /system/lib/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+48)
    #18 pc 00023a5b  /system/lib/libbinder.so
    #19 pc 000104d5  /system/lib/libutils.so (android::Thread::_threadLoop(void*)+112)
    #20 pc 00010045  /system/lib/libutils.so
    #21 pc 000162e3  /system/lib/libc.so (__pthread_start(void*)+30)
    #22 pc 000142d3  /system/lib/libc.so (__start_thread+6)


*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'google/hammerhead/hammerhead:5.0/LRX21O/1570415:user/release-keys'
Revision: '11'
ABI: 'arm'
pid: 21531, tid: 24292, name: Binder_5  >>> /system/bin/surfaceflinger <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x15
    r0 fffffffd  r1 00000000  r2 fffffff0  r3 b6e2fc60
    r4 fffffffd  r5 ae030040  r6 00000000  r7 b46f3330
    r8 000001ec  r9 b6f18df4  sl 00000018  fp 00000000
    ip b6e2ff58  sp ae210a58  lr b6e2d7b5  pc b6d94386  cpsr 000f0030


backtrace:
    #00 pc 00002386  /system/lib/libunwind.so
```

```
    #01 pc 000047b1  /system/lib/libbacktrace.so (UnwindMap::~UnwindMap()+24)
    #02 pc 00004807  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+38)
    #03 pc 0000481d  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+4)
    #04 pc 0000493d  /system/lib/libbacktrace.so (BacktraceMap::Create(int, bool)+76)
    #05 pc 00003155  /system/lib/libbacktrace.so (Backtrace::Backtrace(BacktraceImpl*, int, BacktraceMap*)+52)
    #06 pc 0000317f  /system/lib/libbacktrace.so (BacktraceCurrent::BacktraceCurrent(BacktraceImpl*, BacktraceMap*)+22)
    #07 pc 0000405f  /system/lib/libbacktrace.so (CreateCurrentObj(BacktraceMap*)+28)
    #08 pc 0000cfe3  /system/lib/libutils.so (android::CallStack::update(int, int)+38)
    #09 pc 0000d107  /system/lib/libutils.so (android::CallStack::CallStack(char const*, int)+38)
    #10 pc 00023513  /system/lib/libbinder.so (android::Parcel::read(android::Parcel::FlattenableHelperInterface&) const+246)
    #11 pc 00033035  /system/lib/libgui.so (android::BnGraphicBufferProducer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+568)
    #12 pc 0001a6d9  /system/lib/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+60)
    #13 pc 0001f787  /system/lib/libbinder.so (android::IPCThreadState::executeCommand(int)+582)
    #14 pc 0001f8ab  /system/lib/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+38)
    #15 pc 0001f8ed  /system/lib/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+48)
    #16 pc 00023a5b  /system/lib/libbinder.so
    #17 pc 000104d5  /system/lib/libutils.so (android::Thread::_threadLoop(void*)+112)
    #18 pc 00010045  /system/lib/libutils.so
    #19 pc 000162e3  /system/lib/libc.so (__pthread_start(void*)+30)
    #20 pc 000142d3  /system/lib/libc.so (__start_thread+6)


*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'google/hammerhead/hammerhead:5.0/LRX21O/1570415:user/release-keys'
Revision: '11'
ABI: 'arm'
pid: 22794, tid: 23171, name: Binder_3  >>> /system/bin/surfaceflinger <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x15
    r0 fffffffd  r1 00000000  r2 fffffff0  r3 b6ed2c60
    r4 fffffffd  r5 b251c100  r6 00000000  r7 b25127e0
    r8 0000025f  r9 b6fbbdf4  sl 00000018  fp 00000000
    ip b6ed2f58  sp b270da58  lr b6ed07b5  pc b6e37386  cpsr 000f0030

backtrace:
    #00 pc 00002386  /system/lib/libunwind.so
    #01 pc 000047b1  /system/lib/libbacktrace.so (UnwindMap::~UnwindMap()+24)
    #02 pc 00004807  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+38)
    #03 pc 0000481d  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+4)
    #04 pc 0000493d  /system/lib/libbacktrace.so (BacktraceMap::Create(int, bool)+76)
    #05 pc 00003155  /system/lib/libbacktrace.so (Backtrace::Backtrace(BacktraceImpl*, int, BacktraceMap*)+52)
    #06 pc 0000317f  /system/lib/libbacktrace.so (BacktraceCurrent::BacktraceCurrent(BacktraceImpl*, BacktraceMap*)+22)
    #07 pc 0000405f  /system/lib/libbacktrace.so (CreateCurrentObj(BacktraceMap*)+28)
    #08 pc 0000cfe3  /system/lib/libutils.so (android::CallStack::update(int, int)+38)
    #09 pc 0000d107  /system/lib/libutils.so (android::CallStack::CallStack(char const*, int)+38)
    #10 pc 00023513  /system/lib/libbinder.so (android::Parcel::read(android::Parcel::FlattenableHelperInterface&) const+246)
    #11 pc 00033035  /system/lib/libgui.so (android::BnGraphicBufferProducer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+568)
    #12 pc 0001a6d9  /system/lib/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+60)
    #13 pc 0001f787  /system/lib/libbinder.so (android::IPCThreadState::executeCommand(int)+582)
    #14 pc 0001f8ab  /system/lib/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+38)
    #15 pc 0001f8ed  /system/lib/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+48)
    #16 pc 00023a5b  /system/lib/libbinder.so
    #17 pc 000104d5  /system/lib/libutils.so (android::Thread::_threadLoop(void*)+112)
    #18 pc 00010045  /system/lib/libutils.so
    #19 pc 000162e3  /system/lib/libc.so (__pthread_start(void*)+30)
    #20 pc 000142d3  /system/lib/libc.so (__start_thread+6)


*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
Build fingerprint: 'google/hammerhead/hammerhead:5.0/LRX21O/1570415:user/release-keys'
Revision: '11'
ABI: 'arm'
pid: 12872, tid: 14085, name: Binder_4  >>> /system/bin/surfaceflinger <<<
signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x14
    r0 ffffffff  r1 fffffff4  r2 00000001  r3 b6f71fac
    r4 00000000  r5 ffffff28  r6 00000001  r7 b6f65650
    r8 00000249  r9 0000000c  sl 00000018  fp 00000000
    ip b6deff54  sp b21ff9f8  lr b6f0f7a9  pc b6f45bf8  cpsr 200f0030

backtrace:
    #00 pc 00048bf8  /system/lib/libc.so (ifree+47)
    #01 pc 000127a7  /system/lib/libc.so (free+10)
    #02 pc 0000239b  /system/lib/libunwind.so
    #03 pc 000047b1  /system/lib/libbacktrace.so (UnwindMap::~UnwindMap()+24)
    #04 pc 00004807  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+38)
    #05 pc 0000481d  /system/lib/libbacktrace.so (UnwindMapLocal::~UnwindMapLocal()+4)
    #06 pc 0000493d  /system/lib/libbacktrace.so (BacktraceMap::Create(int, bool)+76)
    #07 pc 00003155  /system/lib/libbacktrace.so (Backtrace::Backtrace(BacktraceImpl*, int, BacktraceMap*)+52)
    #08 pc 0000317f  /system/lib/libbacktrace.so (BacktraceCurrent::BacktraceCurrent(BacktraceImpl*, BacktraceMap*)+22)
    #09 pc 0000405f  /system/lib/libbacktrace.so (CreateCurrentObj(BacktraceMap*)+28)
    #10 pc 0000cfe3  /system/lib/libutils.so (android::CallStack::update(int, int)+38)
    #11 pc 0000d107  /system/lib/libutils.so (android::CallStack::CallStack(char const*, int)+38)
    #12 pc 00023513  /system/lib/libbinder.so (android::Parcel::read(android::Parcel::FlattenableHelperInterface&) const+246)
    #13 pc 00033035  /system/lib/libgui.so (android::BnGraphicBufferProducer::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+568)
    #14 pc 0001a6d9  /system/lib/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+60)
    #15 pc 0001f787  /system/lib/libbinder.so (android::IPCThreadState::executeCommand(int)+582)
    #16 pc 0001f8ab  /system/lib/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+38)
    #17 pc 0001f8ed  /system/lib/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+48)
    #18 pc 00023a5b  /system/lib/libbinder.so
```

```
#19 pc 000104d5 /system/lib/libutils.so (android::Thread::_threadLoop(void*)+112)
#20 pc 00010045 /system/lib/libutils.so
#21 pc 000162e3 /system/lib/libc.so (__pthread_start(void*)+30)
#22 pc 000142d3 /system/lib/libc.so (__start_thread+6)
```

✓ Links (1)

"… to address the issue reported, however our product team has shifted work priority that doesn't include this issue. For now, we will be closing the issue as won't fix obsolete. If this issue currently sti

COMMENTS

en...@google.com <en...@google.com>

Assigned to cf...@google.com.

---

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

I'm not sure why it's crashing, but the unwind is failing, and then the code tries to destroy the UnwindMap it just created.

Is there a log for this too? There is probably something in the log that describes why the unwind is failing. I can simulate this quickly to see if it fails in all cases.

[Deleted User] <[Deleted User]> #3

You mean log cat output around the crash dump? I can get that for you when it decides to crash again...

---

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

Yes, that or take a bugreport and upload that.

[Deleted User] <[Deleted User]> #5

I experience a crash at the same address but with a different strack trace. Is this related?

```
12-12 14:11:17.473  23963-24503/***** A/libc： Fatal signal 11 (SIGSEGV), code 1, fault addr 0x9cb00b0c in tid 24503 (GLThread 2709)
12-12 14:11:17.528    179-179/? I/DEBUG： *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
12-12 14:11:17.528    179-179/? I/DEBUG： Build fingerprint: 'google/hammerhead/hammerhead:5.0/LRX21O/1570415:user/release-keys'
12-12 14:11:17.528    179-179/? I/DEBUG： Revision: '11'
12-12 14:11:17.528    179-179/? I/DEBUG： ABI: 'arm'
12-12 14:11:17.528    179-179/? I/DEBUG： pid: 23963, tid: 24503, name: GLThread 2709  >>> at.blockhausmedien.aezmagazine <<<
12-12 14:11:17.528    179-179/? I/DEBUG： signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x9cb00b0c
12-12 14:11:17.569    179-179/? I/DEBUG： r0 000000e9  r1 9cb00aec  r2 00000001  r3 b6ef1fac
12-12 14:11:17.569    179-179/? I/DEBUG： r4 9cb00000  r5 ffffff28  r6 9cbea040  r7 b6ee5650
12-12 14:11:17.569    179-179/? I/DEBUG： r8 00000001  r9 0000000c  sl 00000002  fp 9cbea040
12-12 14:11:17.569    179-179/? I/DEBUG： ip b5cdcf88  sp 9b7ff670  lr b6e8f7a9  pc b6ec5bf8  cpsr 20070030
12-12 14:11:17.569    179-179/? I/DEBUG： backtrace:
12-12 14:11:17.569    179-179/? I/DEBUG： #00 pc 00048bf8  /system/lib/libc.so (ifree+47)
12-12 14:11:17.569    179-179/? I/DEBUG： #01 pc 000127a7  /system/lib/libc.so (free+10)
12-12 14:11:17.569    179-179/? I/DEBUG： #02 pc 001c7c5f  /system/lib/libart.so (art::JNI::ReleasePrimitiveArrayCritical(_JNIEnv*, _jarray*, void*, int)+558)
12-12 14:11:17.569    179-179/? I/DEBUG： #03 pc 000bff09  /system/lib/libart.so (art::CheckJNI::ReleasePrimitiveArrayCritical(_JNIEnv*, _jarray*, void*, int)+116)
12-12 14:11:17.569    179-179/? I/DEBUG： #04 pc 0006169d  /system/lib/libandroid_runtime.so
12-12 14:11:17.570    179-179/? I/DEBUG： #05 pc 00068c09  /system/lib/libandroid_runtime.so
12-12 14:11:17.570    179-179/? I/DEBUG： #06 pc 00b7e2c1  /data/dalvik-cache/arm/system@framework@boot.oat
```

It happens when launching an OpenGL application that used to run with pre 5.0 Android.

---

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

That last stacktrace is almost certainly memory corruption. It's possible a bug in unwind code is corrupting something, but it does appear that one is something completely different.

---

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

Status: Won't Fix (Obsolete)

Thank you for your feedback. We assure you that we are doing our best to address the issue reported, however our product team has shifted work priority that doesn't include this issue. For n