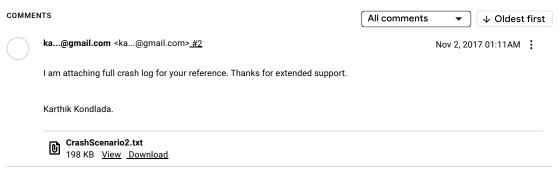Android Public Tracker > App Development > SDK > NDK   68752436

← C ☆ Application getting crash on versifying isInstanceOf method in cpp

+1 2   Hotlists   Mark as Duplicate   🔔   ⋮

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

Can't Repro   Bug   P2   + Add Hotlist

👥 **STATUS UPDATE** No update yet.   Edit

📄 **DESCRIPTION** ka...@gmail.com created issue #1   Nov 2, 2017 01:00AM   ⋮

Hi,

Synopsis :
Application getting crash on explicitly invoking garbage collection to remove native objects.

App Description:
On launch of our application, we have v8 java script engine which will process the javascript input and show the UI.

Scenario:
The issue is happening some times , when a 'garbage collection' is invoked from v8 engine on specific jsobject which is already created.
Observed crash on destructor of an object.

Can you please let me know the reason for the crash , is it really crashed @isInstanceOf method in destructor or for any other reason?

codesnippet ::

```
if(widget != NULL){
    JNIEnv *env = JSUtil::getEnv();
    if(env->IsInstanceOf(widget, JSUtil::JSObjectClz)){
        env->CallVoidMethod(widget,JSUtil::mid_JSObject_setJSObject_J_V,(jlong)0);
    }
    env->DeleteGlobalRef(widget);
}
```

Logs/StackTrace ::
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #00 pc 002c42f7 /system/lib/libart.so
(_ZN3art15DumpNativeStackERNSt3__113basic_ostreamIcNS0_11char_traitsIcEEEEiP12BacktraceMapPKcPNS_9ArtMethodEPv+13
0)
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #01 pc 00355859 /system/lib/libart.so
(_ZNK3art6Thread9DumpStackERNSt3__113basic_ostreamIcNS1_11char_traitsIcEEEEbP12BacktraceMapb+200)
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #02 pc 00351d2b /system/lib/libart.so
(_ZNK3art6Thread4DumpERNSt3__113basic_ostreamIcNS1_11char_traitsIcEEEEbP12BacktraceMapb+34)
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #03 pc 0022f7fd /system/lib/libart.so
(_ZN3art9JavaVMExt8JniAbortEPKcS2_+736)
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #04 pc 0022fc67 /system/lib/libart.so
(_ZN3art9JavaVMExt9JniAbortFEPKcS2_z+66)
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #05 pc 0035978f /system/lib/libart.so
(_ZNK3art6Thread13DecodeJObjectEP8_jobject+350)
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #06 pc 000d1a25 /system/lib/libart.so
(_ZN3art11ScopedCheck13CheckInstanceERNS_18ScopedObjectAccessENS0_12InstanceKindEP8_jobjectb+64)
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #07 pc 000d103f /system/lib/libart.so
(_ZN3art11ScopedCheck22CheckPossibleHeapValueERNS_18ScopedObjectAccessEcNS_12JniValueTypeE+226)
10-31 15:07:53.515: A/zygote(17408): java_vm_ext.cc:504]   native: #08 pc 000d0891 /system/lib/libart.so
(_ZN3art11ScopedCheck5CheckERNS_18ScopedObjectAccessEbPKcPNS_12JniValueTypeE+604)
10-31 15:07:53.516: A/zygote(17408): java_vm_ext.cc:504]   native: #09 pc 000c4ce5 /system/lib/libart.so
(_ZN3art8CheckJNI12IsInstanceOfEP7_JNIEnvP8_jobjectP7_jclass+452)

NDK Version: 'android-ndk-r9d'
compile SDK Version: 15
target SDK Version: 15

COMMENTS

All comments ▼   ↓ Oldest first

⬤ **ka...@gmail.com** <ka...@gmail.com> #2   Nov 2, 2017 01:11AM   ⋮

I am attaching full crash log for your reference. Thanks for extended support.

Karthik Kondlada.

📎 **CrashScenario2.txt**
   198 KB View Download

⬤ **ch...@gmail.com** <ch...@gmail.com> #3   Nov 20, 2017 08:07PM   ⋮

Reporter	⬤ ka...@gmail.com
Type	Bug
Priority	P2
Severity	S2
Status	Won't fix (Not reproducible)
Access	Default access View
Assignee	⬤ ka...@gmail.com
Verifier	--
Collaborators	👥 ⌄
CC	🔒 ⌄
	ag...@google.com
	ar...@google.com
	ka...@gmail.com
	ma...@google.com
AOSP ID	--
ReportedBy	--
Found In	--
Targeted To	--
Verified In	--
In Prod	⬤

Please find the attached bug report.

📎 **bugreport-angler-OPR5.170623.011-2017-11-19-17-42-31.zip**
3.6 MB   Download

---

en...@google.com <en...@google.com>   Feb 1, 2018 05:58AM

Assigned to se...@google.com.

---

ag...@google.com <ag...@google.com> #4   Feb 1, 2018 06:30AM   ⋮

Reassigned to ka...@gmail.com.

10-31 15:07:53.627: A/zygote(17408): runtime.cc:500] JNI DETECTED ERROR IN APPLICATION: use of invalid jobject 0x6500

Are you sure that the jobject is valid? That value definitely doesn't look that way. 0xXYZ0 means it is kHandleScopeOrInvalid.
The last two bits should be 10 for it to really be a global ref. I'd suggest CheckJNI and ASAN or similar, as it looks like your app
has some issues.

---

ag...@google.com <ag...@google.com> #5   Feb 1, 2018 06:31AM   ⋮

(We can't do more without complete source to your project)

---

en...@google.com <en...@google.com>   Mar 19, 2019 06:55AM

Status: Won't Fix (Not Reproducible)