java.nio.SocketChannel finalize crash

+1 Hotlists (2) Mark as Duplicate

Comments (7) Dependencies Duplicates (0) Blocking (0) Resources (3)

Fixed Bug P3 + Add Hotlist [AOSP] assigned

STATUS UPDATE No update yet. Edit

DESCRIPTION sa...@gmail.com created issue #1 Dec 12, 2018 09:43PM

Reopening https://issuetracker.google.com/issues/112575287 as I have encountered the same issue.

I have an application that uses java.nio.Channel.SocketChannel for asynchronous TCP sockets. When there are open sockets and Wi-Fi is changed, the application crashes sometimes. This issue seems to occur 10-20% of the time.

I tried to investigate the cause, and it seems to me that SocketChannelImpl.finalize() causes the crash after calling close() for the SocketChannel and passes a NULL FileDescriptor object to JNI function preClose0. However, when looking at the JDK source code that is included in the Android 9.0.0 Release 16 (PQ1A.181105.017.A1) that the test phone is running, I could not find a finalize() implementation for the sun.nio.ch.SocketChannelImpl class so I could not further investigate the cause.

I have been using the code almost unchanged for a long time and this issue has only found after upgrading one of the test phones to Android 9.0.0.

Please find below answers to the questions posted in the previous issue as well as a link to the bug report.

1) Steps to reproduce:

I can't be exactly sure of the conditions required to reproduce the issue but in my application it can be reproduced by having open java.nio.Channels.SocketChannel connections and chaning the Wi-Fi. I suspect that it is not directly related to the Wi-Fi change and is rather an issue with arbitrary loss of connection and possibly reconnection but so far that has been the only way to reproduce the issue.

2) Frequency:

about 10-20% of times

3) Expected output:

Properly closed socket without issues

4) Current output

Crash when finalize is called

5) Android bug report

https://drive.google.com/file/d/13po8wbTxh0-IUlwhmPXKm_rOH3-kvR7n/view?usp=sharing

✓ Mentioned issues (2) Hide all

P3 JNI DETECTED ERROR IN APPLICATION: field operation on NULL object: 0x0 "https://issuetracker.google.com/112575287" sa...@ #1

P3 JNI DETECTED ERROR IN APPLICATION: field operation on NULL object: 0x0 "https://issuetracker.google.com/114626790" sa...@ #4

COMMENTS All comments ↓ Oldest first

ve...@google.com <ve...@google.com> #2 Dec 12, 2018 10:05PM

Assigned to ve...@google.com.

Thank you for reporting this issue. For us to further investigate this issue, please provide the following additional information:

Please provide sample project or apk to reproduce the issue. Also mention the steps to be followed for reproducing the issue with the given sample project or apk.

Screen capture of the issue
Press the volume down and power buttons simultaneously. The image will appear in your gallery. Attach the screenshot file to this issue.

Screen record of the issue, for clarity
Please capture screen record or video of the issue using following steps:
adb shell screenrecord /sdcard/video.mp4
Subsequently use following command to pull the recorded file:
adb pull /sdcard/video.mp4
Attach the file to this issue.

Note: Please upload the files to google drive and share the folder to android-bugreport@google.com, then share the link here.

Reporter	sa...@gmail.com
Type	Bug
Priority	P3
Severity	S3
Status	Fixed
Access	Default access View
Assignee	ve...@google.com
Verifier	--
Collaborators	
CC	sa...@gmail.com
AOSP ID	--
ReportedBy	--
Found In	--
Targeted To	--
Verified In	--
In Prod	

sa...@gmail.com <sa...@gmail.com> #3 Dec 15, 2018 02:08AM

Hi,

so far I haven't been able to reproduce the issue in a simple sample application. Our apk is not useful for you since our application logic relies heavily on a specific type of other device being in the network.

The crash happens as a part of a device setup process, where the device that is being setup hosts a wifi network and the Android device connects to the hotspot and sends certain configuration information. When the setup is completed, the device silently shuts down the wifi hotspot without sending TCP FIN or RST and connects to a wifi network provided during the setup process. At this point the Android device will automatically switch to a known network because the previous network disappears but in this point the crash sometimes occurs. I assume that the crash is caused by the connections that are terminated due to I/O errors after the network change but the Android device initiates other connections immediately after connecting to the known wifi. However, since the crash stack trace only points to the finalize() I haven't been able to verify which connection is causing the crash.

The device setup process only uses HTTP through OkHttp library which is in turn using java.nio. After the wifi is changed, java.nio is used directly for raw TCP connections.

I updated the test phone to build PQ1A.181205.002 today and verified that the crash still happens.

Even though I am not able to provide you a sample (unless I figure out a way to reproduce this in a sample environment), is it possible that you could investigate the issue based on this information? I would also be interested to take a look at the source code of the sun.nio implementations that are running on the device. Is that source code available somewhere?

---

sa...@gmail.com <sa...@gmail.com> #4 Dec 17, 2018 08:53PM

I noticed that there's a followup ticket to the one I linked, with a sample that reproduces the issue: https://issuetracker.google.com/issues/114626790.

---

ve...@google.com <ve...@google.com> #5 Dec 19, 2018 05:30PM

We have passed this to the development team and will update this issue with more information as it becomes available.

---

sa...@gmail.com <sa...@gmail.com> #6 Dec 20, 2018 01:55AM

It looks to me like SocketChannelImpl constructor throws and leaves the object in a broken state where the FileDescriptor object is null. Then finalizer tries to cleanup the broken object and blows. Here's a stacktrace of an exception thrown by SocketChannel.open() just before the crash.

```
java.net.SocketException: Machine is not on the network
    at sun.nio.ch.Net.socket0(Native Method)
    at sun.nio.ch.Net.socket(Net.java:420)
    at sun.nio.ch.Net.socket(Net.java:413)
    at sun.nio.ch.SocketChannelImpl.<init>(SocketChannelImpl.java:130)
    at sun.nio.ch.SelectorProviderImpl.openSocketChannel(SelectorProviderImpl.java:60)
    at java.nio.channels.SocketChannel.open(SocketChannel.java:145)
```

---

vi...@google.com <vi...@google.com> #7 May 22, 2019 10:02PM

Marked as fixed.

Thanks for reporting this bug which was present in Android for several years.

Prior to Android P it was harmless, but an unrelated change in P causes it to crash in native code. The bug is fixed in the public Q betas.

On Android P you can work around it by avoiding calls to ConnectivityManager.bindProcessToNetwork()