SDP can hang if the RFCOMM socket is closed before discovery completes

+1 7 Hotlists (5) Mark as Duplicate

Comments (10) Dependencies Duplicates (0) Blocking (0) Resources (2)

Infeasible Bug P3 + Add Hotlist NeedsInfo

STATUS UPDATE No update yet. Edit

DESCRIPTION jo...@gmail.com created issue #1

This is in Android 12 when implementing CarPlay...

See the following log. (Note this issue isn't easy to reproduce so I'm not providing a bugreport.)

```
68712 2022/10/09 03:10:02.015816 13362.5649 226 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/BluetoothTransport[37827]: open
68793 2022/10/09 03:10:02.052424 13362.6047 227 MGUA ALD LCAT 444 log info verbose 2 bt_btif_dm[40208]: system/bt/btif/src/btif_dm.cc:1920 btif_dm_cancel_discovery: Cancel search
68794 2022/10/09 03:10:02.052510 13362.6047 228 MGUA ALD LCAT 444 log info verbose 2 bt_btm[40208]: system/bt/main/bte_logmsg.cc:198 LogMsg: BTM_CancelRemoteDeviceName()
68820 2022/10/09 03:10:02.055546 13362.6063 236 MGUA ALD LCAT 444 log info verbose 2 bt_sdp[40208]: system/bt/main/bte_logmsg.cc:198 LogMsg: sdp_conn_originate: SDP - Originate s
80456 2022/10/09 03:10:07.009546 13367.5618 161 MGUA ALD LCAT 444 log warn verbose 2 #IAP/SERVICE/IapConnection[37827]: Exception waiting for open()
      at com.bmwgroup.idnext.iap.connection.IapConnection.open(IapConnection.java:185)
-- 5 second CarPlay initial timeout - the Bluetooth socket isn't closed, so it is still attempting to connect.

87970 2022/10/09 03:10:10.249109 13370.8012 56 MGUA ALD LCAT 444 log info verbose 2 bluetooth[40208]: system/bt/stack/rfcomm/rfc_mx_fsm.cc:79 rfc_mx_sm_execute: RFCOMM peer:x
-- Sets state to RFC_MX_STATE_DISC_WAIT_UA and starts 3 second timer.
-- Calls rfc_send_disc

95202 2022/10/09 03:10:13.248095 13373.8005 200 MGUA ALD LCAT 444 log info verbose 2 bluetooth[40208]: system/bt/stack/rfcomm/rfc_mx_fsm.cc:79 rfc_mx_sm_execute: RFCOMM peer:
-- Releases multiplexer control block but doesn't call any callbacks

96879 2022/10/09 03:10:14.025061 13374.5773 212 MGUA ALD LCAT 444 log info verbose 2 bt_sdp[40208]: system/bt/main/bte_logmsg.cc:198 LogMsg: SDP - Rcvd L2CAP disc, CID: 0x56
-- sdp_disconnect_ind received - p_cb2 called with status (either SDP_SUCCESS or SDP_CONN_FAILED) and slot ID.  (p_cb2 is bta_jv_start_discovery_cback in this case)
-- if p_ccb->con_state == SDP_STATE_CONNECTED, then the status is SDP_SUCCESS, otherwise SDP_CONN_FAILED.
-- bta_jv_start_discovery_cback calls:
  -- jv_dm_cback with event BTA_JV_DISCOVERY_COMP_EVT and status BTA_JV_SUCCESS or BTA_JV_FAILURE (depending on above status).
     -- jv_dm_cback calls find_rfc_slot_by_id(id) which succeeds.
     -- If status is BTA_JV_SUCCESS (which should be the case since the state is RFC_MX_STATE_CONNECTED).
       -- The callback calls BTA_JvRfcommConnect which then calls bta_jv_rfcomm_connect in the main thread which then calls rfcomm_cback with the event BTA_JV_RFCOMM_CL_INIT_EVT
         -- rfcomm_cback calls on_cl_rfc_init which calls find_rfc_slot_by_id(id) which fails (see below).
     -- calls cleanup_rfc_slot if there is an error in send_app_scn(slot) (which causes the exception below and the find_rfc_slot_by_id to fail).
  -- find_rfc_slot_by_pending_sdp() to start any pending SDP requests.

96880 2022/10/09 03:10:14.025249 13374.5773 213 MGUA ALD LCAT 444 log error verbose 2 bt_btif_sock_rfcomm[40208]: system/bt/btif/src/btif_sock_rfc.cc:155 find_rfc_slot_by_id: find_rfc_

96895 2022/10/09 03:10:14.025855 13374.5774 228 MGUA ALD LCAT 444 log error verbose 2 #IAP/SERVICE/BluetoothTransport[37827]: An exception was thrown while connecting to the RFC(

96900 2022/10/09 03:10:14.026558 13374.5774 233 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/BluetoothTransport[37827]: close()
-- close() has no effect since the socket has already been closed by the Bluetooth stack.

96912 2022/10/09 03:10:14.027423 13374.5775 245 MGUA ALD LCAT 444 log warn verbose 2 #IAP/JNI[37827]: packages/services/bmw/iap/service/lib/iAP2BMW/transport/Transport.cpp:21(
-- Going into a retry loop.

98056 2022/10/09 03:10:14.525226 13375.0777 146 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/BluetoothTransport[37827]: open
98076 2022/10/09 03:10:14.535587 13375.0882 147 MGUA ALD LCAT 444 log info verbose 2 bt_btif_dm[40208]: system/bt/btif/src/btif_dm.cc:1920 btif_dm_cancel_discovery: Cancel search
98079 2022/10/09 03:10:14.536620 13375.0893 148 MGUA ALD LCAT 444 log info verbose 2 bt_sdp[40208]: system/bt/main/bte_logmsg.cc:198 LogMsg: sdp_conn_originate: SDP - Originate s
-- Originate started for orignal device (8c:41)

101404 2022/10/09 03:10:15.802051 13376.3547 36 MGUA ALD LCAT 444 log info verbose 2 bt_sdp[40208]: system/bt/main/bte_logmsg.cc:198 LogMsg: sdp_conn_originate: SDP - Originate s
-- Originate started for another device (bd:39) even though one is already in progress.

149946 2022/10/09 03:10:35.808731 13396.3455 82 MGUA ALD LCAT 444 log info verbose 2 bluetooth[40208]: system/bt/stack/rfcomm/rfc_mx_fsm.cc:79 rfc_mx_sm_execute: RFCOMM peer:
-- The same sequence as above for device 8c:41 happens for bd:39.
-- Sets state to RFC_MX_STATE_DISC_WAIT_UA and starts 3 second timer.
-- Calls rfc_send_disc

157004 2022/10/09 03:10:38.792209 13399.3453 107 MGUA ALD LCAT 444 log info verbose 2 bluetooth[40208]: system/bt/stack/rfcomm/rfc_mx_fsm.cc:79 rfc_mx_sm_execute: RFCOMM pee
-- Releases multiplexer control block but doesn't call any callbacks

164598 2022/10/09 03:10:41.998896 13402.5525 36 MGUA ALD LCAT 444 log info verbose 2 #CARPLAY/APP/IapOverBluetoothConnectionRepository[38710]: close()
164599 2022/10/09 03:10:41.999041 13402.5526 37 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/ControlSessionManagerImpl[37827]: destroy connection: transportType = BLUETOO
-- Second CarPlay timeout. (Note that we're no longer getting any logs from the lower level Bluetooth stack.)

164644 2022/10/09 03:10:42.013123 13402.5657 44 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/BluetoothTransport[37827]: close()
-- Close from CarPlay

164653 2022/10/09 03:10:42.013643 13402.5659 53 MGUA ALD LCAT 444 log error verbose 2 bt_btif_sock_rfcomm[40208]: system/bt/btif/src/btif_sock_rfc.cc:851 btsock_rfc_signaled: btsock
-- This is a result of the socket being closed.
-- Note: This doesn't cause the waiting originate to be started. THIS IS A BUG IN THE CODE.

164654 2022/10/09 03:10:42.013949 13402.5662 54 MGUA ALD LCAT 444 log warn verbose 2 #IAP/JNI[37827]: packages/services/bmw/iap/service/lib/iAP2BMW/transport/Transport.cpp:21(
-- Note that although we are shutting down the overall connection, the retry thread is still running and trying to reconnect.

165614 2022/10/09 03:10:42.488731 13403.0423 222 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/BluetoothTransport[37827]: open
165627 2022/10/09 03:10:42.496413 13403.0499 223 MGUA ALD LCAT 444 log info verbose 2 bt_btif_dm[40208]: system/bt/btif/src/btif_dm.cc:1920 btif_dm_cancel_discovery: Cancel search
-- We don't try to do an Originate because one is already in progress.  A slot is created and marked "pending".

165629 2022/10/09 03:10:42.498964 13403.0526 224 MGUA ALD LCAT 444 log error verbose 2 bt_btif_sock_rfcomm[40208]: system/bt/btif/src/btif_sock_rfc.cc:155 find_rfc_slot_by_id: find_rfc
-- The close (above) isn't clearing the sdp_active flag so it returns an error immediately and doesn't even try to do an SDP Originate. THIS IS A SECOND BUG.

165630 2022/10/09 03:10:42.499071 13403.0526 225 MGUA ALD LCAT 444 log error verbose 2 #IAP/SERVICE/BluetoothTransport[37827]: An exception was thrown while connecting to the RFC

165632 2022/10/09 03:10:42.499127 13403.0526 227 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/BluetoothTransport[37827]: close()
-- Note this has no effect since the socket has already been closed.

165634 2022/10/09 03:10:42.499206 13403.0527 229 MGUA ALD LCAT 444 log warn verbose 2 #IAP/JNI[37827]: packages/services/bmw/iap/service/lib/iAP2BMW/transport/Transport.cpp:2
-- Note that again, although we are shutting down, the retry thread is still running and trying to reconnect.

167026 2022/10/09 03:10:43.001140 13403.5523 179 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/IapConnectionThreadPool(BLUETOOTH)[37827]: ThreadPool is terminated
167033 2022/10/09 03:10:43.003476 13403.5570 180 MGUA ALD LCAT 444 log info verbose 2 #IAP/SERVICE/ControlSessionManagerImpl[37827]: Connection was removed 08:87:C7:82:8C:41
-- Finally the thread is shut down.

-- Note that after this all RFCOMM connection attempts will fail because there is a request that is already waiting to be processed that will never be processed or the sdp_active flag is set and is 
```

✓ Links (1)

" …"issue isn't easy to reproduce so I'm not providing a bugreport". If by any chance you manage to capture a full bugreport, please share it with us. Android bug report (to be captured after reproducing

COMMENTS

fk...@gmail.com <fk...@gmail.com> #2

Mobile screen hinging in game mode

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

Assigned to vi...@google.com.

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

Android build
Which Android build are you using? (e.g. PPP5.180610.010)

Device used -- Device Make, Model, Android OS Version
Which device did you use to reproduce this issue?

Steps to reproduce
What steps are needed to reproduce this issue? Explain a bit more in detail.

We've noted the comment "*issue isn't easy to reproduce so I'm not providing a bugreport*". If by any chance you manage to capture a full bugreport, please share it with us. Android bug report

Note: Please avoid uploading directly to the issue using attachments. You may upload to google drive and share the folder to android-bugreport@google.com, then share the link here.

jo...@gmail.com <jo...@gmail.com> #4

Android build is 12.0.0_r28 SQ1A.220205.002
Device is iPhone 13 with IOS 15.5

The steps to reproduce are outlined in the original post.
It requires doing some programming to reproduce since this is an implementation of CarPlay.
I think doing the following should reproduce the issue.
1) Call createRfccommSocketToServiceRecord(UUID.fromString("00000000-deca-fade-deca-deafdecacafe")) // This is the Wireless iAP2 UUID
2) Close the created socket before SDP completes. This causes the btsock_rfc_signaled code to execute which shuts down the RFCOMM slot and closes the socket. That means when SDP
3) Do the above step 1) again. This should hang since there is already a request in progress that can now never complete.

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

Thanks for the above information. Could you please provide a sample project or apk to reproduce the issue.

ru...@gmail.com <ru...@gmail.com> #6

Can you attach an image file to the platform?

Screenshot_20230314-132932.png
66 KB View Download ?

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

As requested in comment#5, please share a sample project or apk to reproduce the issue.

jo...@gmail.com <jo...@gmail.com> #8

I haven't had time to do that yet... It's on my list.

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

Please provide the requested information to proceed further. Unfortunately the issue will be closed within 7 days if there is no further update.

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

Status: Won't Fix (Infeasible)

We are closing this issue as we don't have enough actionable information. If you are still facing this problem, please open new issue and add the relevant information along with reference to