

BEEM - Android XMPP - Bug #561

NullPointerException (NPE) in Beem Android XMPP

08/14/2014 08:48 PM - Danilo Dominguez

Status:	New	Start date:	08/14/2014
Priority:	High	Due date:	
Assignee:		% Done:	0%
Category:	XMPP	Estimated time:	0.00 hour
Target version:		Locale:	
Affected version:	0.1.8		
Description			
Dear Beem Team,			
<p>I have implemented an static analysis tool for finding bugs in Android apps and I have found a NullPointerException (NPE) in the following class of your app:</p> <p>- com.beem.project.beem.ui.Chat</p> <p>What steps will reproduce the problem?</p> <ol style="list-style-type: none">1. Open the app with an account set up (I am using a google account).2. Open a chat activity with a friend from your contact list.3. Tab the menu button.4. Tab OTR actions.5. Tab the home button and before the window closes, tab Start OTR session. <p>This will create a NPE in the Chat activity. It is worth to mention that there are other scenarios in which this bug can be seen. For example, if the user repeat the first 4 steps and receives a phone call, but before the phone call activity takes the foreground, the user tabs in the option Start OTR session. This creates a race condition between the callbacks onPause and onOptionsItemSelected (onPause is called before onOptionsItemSelected). Other apps have had this problem as you can see in bug found in MyTracks [1].</p> <p>To be more precise, mChatManager is set to null in onPause and then dereference in onOptionsItemSelected in:</p> <pre>try { if (mChat == null) { mChat = mChatManager.createChat(mContact, mMessageListener); if (mChat != null) { mChat.setOpen(true); } } mChat.startOtrSession(); } catch (RemoteException e) { Log.e(TAG, "start otr chats failed " + mChat, e); }</pre> <p>To fix this problem check if the field mChatManager is not null in the callback onOptionsItemSelected.</p> <pre>try { if (mChat == null && mChatManager != null) { mChat = mChatManager.createChat(mContact, mMessageListener); if (mChat != null) { mChat.setOpen(true); } } mChat.startOtrSession(); } } catch (RemoteException e) { Log.e(TAG, "start otr chats failed " + mChat, e); }</pre> <p>What is the expected output? What do you see instead</p> <p>The app crashes. The app must not crash and maintain the same state when the user comeback to the app.</p> <p>What version of Beem are you using? On what Android version? On what device?</p> <p>Beem 0.1.8 on a Samsung S4 Mini with Android 4.2.2.</p>			

Please provide any additional information below.

[1]

<https://code.google.com/p/mytracks/issues/detail?id=741&can=1&q=status%3AFixed&sort=id&colspec=ID%20Type%20Component%20Status%20Priority%20Targeting%20Work%20Stars%20Owner%20Summary&start=200>

History

#1 - 08/20/2014 04:47 PM - Danilo Dominguez

This behavior also happens in the class `com.beem.project.beem.ui.ContactList` with the field `mXmppFacade`.

Check case:

case `R.id.contact_list_context_menu_call_item` in `onContextItemSelected` and check if `mXmppFacade != null`