

Search IssueTracker

Sign in

Android Public Tracker36937227

←

↺

☆

Android 4.0 Webview Javascript to Java Bridge breaks during onActivityResultResult

+1²

Hotlists (1)

Mark as Duplicate

🔔

⋮

Comments (11)

Dependencies

Duplicates (0)

Blocking (0)

Resources (5)

Obsolete

Bug

P3

+ Add Hotlist

NeedsInfo

👤

STATUS UPDATE

No update yet.

Edit

📄

DESCRIPTION

ma...@gmail.com created issue #1

Hi, while testing our web app on ICS on a galaxy nexus and nexus s, we discovered a bug involving a webview running javascript that triggers a new activity via startActivityForResult(). This activi through onActivityResult(). Once the webview activity becomes active again, the Javascript bridge is completely broken. No more calls to execute javascript through webview.loadUrl("javascript: This is not the case on 1.6 - 3.2. It works as expected. If you have any advice to help us, this is a critical part of our application.

✓

Mentioned issues (1)

✓

Links (4)

🔖

Mentioned issues (1)

P2

Many overseas apps crash when launched on Android T devices

"From [issue 273883685](#) on 22.03.2023:"

🔗

Links (4)

"See [http://developer.android.com/reference/android/webkit/WebView.html#addJavascriptInterface\(java.lang.Object, java.lang.String\)](http://developer.android.com/reference/android/webkit/WebView.html#addJavascriptInterface(java.lang.Object, java.lang.String)) and <http://developer.android.com/guide/topics/fundamentals/>

"See [http://developer.android.com/reference/android/webkit/WebView.html#addJavascriptInterface\(java.lang.Object, java.lang.String\)](http://developer.android.com/reference/android/webkit/WebView.html#addJavascriptInterface(java.lang.Object, java.lang.String)) and <http://developer.android.com/guide/topics/fundamentals/>

"[http://webview.post](#)"

"...ensions is loaded dynamically. It is declared as a dependency using the <uses-library> tag [COMMENTS

en...@google.com

<en...@google.com>

Assigned to st...@google.com.

st...@google.com

<st...@google.com>

#2

Status: New

Hi, thanks for the report.

We use 'Java Bridge' to refer to the WebView's ability to allow JavaScript to invoke Java code, through use of WebView.addJavascriptInterface\(\). However, it sounds like the problem you're de

It sounds like calls to WebView.loadUrl\("javascript:<script>"\) are not working under some circumstances. Is JavaScript working at all in the WebView in these cases? For example, if you have e

Can you send a minimal code snippet that repros the problem?

ma...@gmail.com

<ma...@gmail.com>

#3

12-20 10:17:12.757: DEBUG/CommandHandler\(4987\): displayTextInput {"hint":"Your message","canceltext":"Cancel","text":"","title":"Compose","donetext":"Send"}
12-20 10:17:12.757: DEBUG/MainActivity\(4987\): displayTextInput\(\) for TextInputActivity
12-20 10:17:12.757: INFO/ActivityManager\(178\): START {cmp=*package*/.TextInputActivity \(has extras\)} from pid 4987
12-20 10:17:12.835: DEBUG/dalvikvm\(178\): JIT code cache reset in 7 ms \(1048508 bytes 2/0\)
12-20 10:17:12.843: DEBUG/dalvikvm\(178\): GC_FOR_ALLOC freed 218K, 10% free 19445K/21383K, paused 50ms
12-20 10:17:12.843: INFO/dalvikvm-heap\(178\): Grow heap \(frag case\) to 19.284MB for 230416-byte allocation
12-20 10:17:12.882: DEBUG/dalvikvm\(178\): GC_FOR_ALLOC freed 33K, 10% free 19637K/21639K, paused 36ms
12-20 10:17:12.882: DEBUG/CommandHandler\(4987\): Call to "displayTextInput" was handled.
12-20 10:17:12.945: DEBUG/MainActivity\(4987\): onPause\(\) called
12-20 10:17:12.991: DEBUG/dalvikvm\(4987\): GC_EXPLICIT freed 359K, 49% free 19137K/36807K, paused 2ms+9ms
12-20 10:17:13.023: INFO/WindowManager\(178\): createSurface Window{41aa56d8 InputMethod paused=false}: DRAW NOW PENDING
12-20 10:17:13.101: INFO/WindowManager\(178\): createSurface Window{41c5d340 *package*/*package*.TextInputActivity paused=false}: DRAW NOW PENDING
12-20 10:17:13.382: INFO/ActivityManager\(178\): Displayed *package*/.TextInputActivity: +386ms
12-20 10:17:26.874: INFO/WindowManager\(178\): createSurface Window{41aa56d8 InputMethod paused=false}: DRAW NOW PENDING
12-20 10:17:29.109: DEBUG/dalvikvm\(178\): GC_FOR_ALLOC freed 694K, 11% free 19434K/21639K, paused 48ms
12-20 10:17:29.124: DEBUG/TextAct onPause\(\)\(4987\): ON PAUSE CALLED
12-20 10:17:29.132: DEBUG/MainActivity\(4987\): onActivityResult\(\) for TextInputActivity
12-20 10:17:29.132: DEBUG/MyWebView\(4987\): Loading URL: javascript:Compose.compose_cb\({"text":"Ggg","backpressed":"false"}\);
12-20 10:17:29.140: DEBUG/MyWebView\(4987\): Loading URL: javascript:applicationDidBecomeActive_cb\(\);
12-20 10:17:29.179: INFO/WindowManager\(178\): createSurface Window{41c02f20 *package*/*package*.MainActivity paused=false}: DRAW NOW PENDING

This is the log from where this seems to happen. I get a json object from the javascript, and make a call to displayTextInput\(\), which is a java function to start our TextInputActivity. When fini](https://cs.android.com/androidx/platform/frameworks/support/+/androidx-main:window/window/src/m</div></div></div><div data-bbox=)

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

> I get a json object from the javascript, and make a call to displayTextInput(), which is a java function
How do you get the result of the JavaScript evaluation to Java? Are you using the Java Bridge (WebView.addJavascriptInterface()) ?

Can you provide a code snippet which repros this, or at least a complete burp report?

ma...@gmail.com <ma...@gmail.com> #5

Yes, to get the result of the JS to Java, we use the Java Bridge.

OnCreate() of MainActivity:

```
mWeb = (MyWebView) findViewById(R.id.web);
mWeb.addJavascriptInterface(
    new MyJSInterface(), "external");
```

The onclick event in the html textarea calls this javascript function:

```
displayTextInput: function(params) {
    window.external.Notify(**JSON string**);
    //calls MyJSInterface.Notify(String json); where the json string is parsed and makes a call to displayTextInput() on the java side.
}
```

Java side displayTextInput():

```
void displayTextInput(JSONObject params, String callback) {
    Log.d(TAG, "displayTextInput() for TextInputActivity");
    Intent intent = new Intent(this, TextInputActivity.class);

    String hint = params.optString("hint", null);
    if (!TextUtils.isEmpty(hint)) {
        intent.putExtra(TextInputActivity.EXTRA_HINT, hint);
    }

    String donetext = params.optString("donetext", null);
    if (!TextUtils.isEmpty(donetext)) {
        intent.putExtra(TextInputActivity.EXTRA_DONETEXT, donetext);
    }

    String text = params.optString("text", null);
    if (!TextUtils.isEmpty(text)) {
        intent.putExtra(TextInputActivity.EXTRA_TEXT, text);
    }

    String threadId = params.optString("threadid", "");
    intent.putExtra(TextInputActivity.EXTRA_THREADID, threadId);
    String receiver = params.optString("receiver", "");
    intent.putExtra(TextInputActivity.EXTRA_RECEIVER, receiver);

    intent.putExtra(TextInputActivity.EXTRA_CALLBACK, callback);

    startActivityForResult(intent, TEXTINPUT_ACTIVITY);
}

onActivityResult():
switch (req) {
    case TEXTINPUT_ACTIVITY:
        Log.d(TAG, "OnActivityResult() for TextInputActivity");
        if (ret == RESULT_OK) {
            String cb = data.getStringExtra(
                TextInputActivity.EXTRA_CALLBACK);
            Map<String, String> args = new HashMap<String, String>();
            String text = data.getStringExtra(TextInputActivity.EXTRA_TEXT);
            final String threadId = data.getStringExtra(TextInputActivity.EXTRA_THREADID);
            final String receiver = data.getStringExtra(TextInputActivity.EXTRA_RECEIVER);
            final String origText = text;
            final boolean backpressed = data.getBooleanExtra(TextInputActivity.EXTRA_BACKPRESSED, false);
            text = text.replace("\\", "\\\\");
            text = text.replaceAll("\\n", "\\\\n")
                .replaceAll("\\r", "\\\\r");

            args.put("text", text);
            args.put("okc_backpressed", String.valueOf(backpressed));
            mWeb.callBack(cb, args);
        }
}
```

mWeb.callBack(cb,args) calls loadUrl("javascript: *cb(*args);"); which refers to this line

12-20 10:17:29.132: DEBUG/MyWebView(4987): Loading URL: javascript:Compose.compose_cb({"text":"Ggg","backpressed":"false"});

There are no errors that show up in the log after:

12-20 10:17:29.179: INFO/WindowManager(178): createSurface Window{41c02f20 *package*/package*.MainActivity paused=false}: DRAW NOW PENDING

I also ran the debugger and checked the webView object after this point. mJavaScriptEnabled = true and any JS interfaces added are still around.

st...@google.com <st...@google.com> [#6](#)

When MyJSInterface.Notify() receives the string from JavaScript, are you switching to the UI thread before calling startActivityForResult()? Calls to objects injected into the WebView using the thread.

See [http://developer.android.com/reference/android/webkit/WebView.html#addJavascriptInterface\(java.lang.Object, java.lang.String\)](http://developer.android.com/reference/android/webkit/WebView.html#addJavascriptInterface(java.lang.Object, java.lang.String)) and <http://developer.android.com/guide/topics/fundamentals>

ma...@gmail.com <ma...@gmail.com> [#7](#)

So sorry for the confusion.

displayTextInput() and therefore startActivityForResult() are both called on the UI thread.

st...@google.com <st...@google.com> [#8](#)

OK, I'll have to look into this more carefully. Can you send the source for a minimal (but complete) app that reproduces the problem?

ma...@gmail.com <ma...@gmail.com> [#9](#)

I could not duplicate the javascript breaking with a minimal app. However, I was able to have the app go to background from pressing 'home', and have onDestroy() called unexpectedly. When

WARN/InputManagerService(175): Starting input on non-focused client com.android.internal.view.IInputMethodClient\$Stub\$Proxy@41b27700 (uid=10059 pid=8710)

This is the line that would always get called before the or any activity died where pid was the process id that would get destroyed. It doesn't always happen, and I have no clue why.


The attached app code is compiled with API level 8.


Example Run: API level 8 running on unlocked Galaxy Nexus

```
=====
12-20 20:49:01.617: INFO/ActivityManager(175): Start proc com.example for activity com.example/.MyActivity: pid=9169 uid=10059 gids={3003, 1015}
12-20 20:49:01.625: DEBUG/Finsky(9118): [1159] DownloadRecords.initializeAndPrune: Pruned 0 old downloads from the cursor.
12-20 20:49:01.625: DEBUG/dalvikvm(9169): Late-enabling CheckJNI
12-20 20:49:01.632: DEBUG/dalvikvm(9154): GC_CONCURRENT freed 537K, 5% free 14308K/14919K, paused 2ms+2ms
12-20 20:49:01.656: VERBOSE/PhoneStatusBar(315): setLightsOn(true)
12-20 20:49:01.726: INFO/ActivityManager(175): Process com.android.keychain (pid 9074) has died.
12-20 20:49:01.734: INFO/WindowManager(175): createSurface Window{4196c7e0 com.example/com.example.MyActivity paused=false}: DRAW NOW PENDING
12-20 20:49:01.750: DEBUG/dalvikvm(9154): GC_CONCURRENT freed 537K, 5% free 14308K/14919K, paused 2ms+2ms
12-20 20:49:01.757: INFO/ActivityThread(9154): Pub com.google.plus.platform: com.google.android.apps.plus.content.AdsProvider
12-20 20:49:01.789: DEBUG/OpenGLRenderer(7829): Flushing caches (mode 1)
12-20 20:49:01.796: DEBUG/OpenGLRenderer(7829): Flushing caches (mode 0)
12-20 20:49:01.804: INFO/ActivityManager(175): Process com.google.android.gallery3d (pid 9061) has died.
12-20 20:49:01.820: VERBOSE/PicasaContentProvider(9154): querySettings: defaults: {sync_on_wifi_only=1, auto_upload_account_type=null, sync_on_battery=1, sync_on_roaming=0, sync_pl
12-20 20:49:01.851: VERBOSE/PhoneStatusBar(315): setLightsOn(true)
12-20 20:49:01.875: DEBUG/dalvikvm(9154): GC_FOR_ALLOC freed 158K, 4% free 14425K/14919K, paused 18ms
12-20 20:49:01.882: DEBUG/UploadsManager(9154): load newPhotoTracker: null
12-20 20:49:01.882: DEBUG/UploadsManager(9154): load all accounts: null
12-20 20:49:01.882: DEBUG/UploadsManager(9154): load all account-album pairs: null
12-20 20:49:01.882: VERBOSE/PicasaContentProvider(9154): querySettings: defaults: {sync_on_wifi_only=1, auto_upload_account_type=null, sync_on_battery=1, sync_on_roaming=0, sync_pl
12-20 20:49:01.882: DEBUG/PicasaSync(9154): sync account database
12-20 20:49:01.898: INFO/ActivityManager(175): Start proc com.android.voicedialer for broadcast com.android.voicedialer/.VoiceDialerReceiver: pid=9193 uid=10055 gids={3002}
12-20 20:49:01.937: DEBUG/PicasaSync(9154): accounts in DB=0
12-20 20:49:01.937: VERBOSE/PicasaContentProvider(9154): querySettings: defaults: {sync_on_wifi_only=1, auto_upload_account_type=null, sync_on_battery=1, sync_on_roaming=0, sync_pl
12-20 20:49:01.945: INFO/ActivityManager(175): Start proc com.android.contacts for broadcast com.android.contacts/.quickcontact.PackageIntentReceiver: pid=9205 uid=10000 gids={300
12-20 20:49:02.039: INFO/ActivityManager(175): Start proc com.google.android.gallery3d for broadcast com.google.android.gallery3d/com.android.gallery3d.app.PackagesMonitor: pid=921
12-20 20:49:02.054: DEBUG/AccountTypeManager(9205): Registering 1 extension packages
12-20 20:49:02.062: ERROR/ExternalAccountType(9205): Unsupported attribute readOnly
12-20 20:49:02.070: DEBUG/AccountTypeManager(9205): Registering extension package account type=com.google, dataSet=plus, packageName=com.google.android.apps.plus
12-20 20:49:02.078: INFO/AccountTypeManager(9205): Loaded meta-data for 3 account types, 0 accounts in 51ms(wall) 20ms(cpu)
12-20 20:49:02.093: INFO/ActivityThread(9219): Pub com.google.android.gallery3d.GooglePhotoProvider: com.google.android.picasasync.PicasaContentProvider
12-20 20:49:02.156: DEBUG/dalvikvm(9219): GC_CONCURRENT freed 414K, 4% free 14112K/14599K, paused 2ms+2ms
12-20 20:49:02.187: INFO/ActivityThread(9219): Pub com.google.android.gallery3d.provider: com.android.gallery3d.provider.GalleryProvider
12-20 20:49:02.242: DEBUG/dalvikvm(9219): GC_CONCURRENT freed 398K, 4% free 14170K/14663K, paused 2ms+2ms
12-20 20:49:02.273: INFO/ActivityManager(175): Displayed com.example/.MyActivity: +678ms
12-20 20:49:02.390: INFO/ActivityManager(175): Start proc com.google.android.partnersetup for broadcast com.google.android.partnersetup/.RlzPingBroadcastReceiver: pid=9232 uid=100
12-20 20:49:02.429: DEBUG/dalvikvm(118): GC_EXPLICIT freed 37K, 3% free 14022K/14339K, paused 2ms+2ms
12-20 20:49:02.429: INFO/ActivityThread(9232): Pub com.google.android.partnersetup.rlzprovider: com.google.android.partnersetup.RlzProvider
12-20 20:49:02.437: INFO/ActivityThread(9232): Pub com.google.android.partnersetup.rlzappprovider: com.google.android.partnersetup.RlzAppProvider
12-20 20:49:02.460: DEBUG/dalvikvm(118): GC_EXPLICIT freed <1K, 3% free 14022K/14339K, paused 2ms+1ms
12-20 20:49:02.492: DEBUG/dalvikvm(118): GC_EXPLICIT freed <1K, 3% free 14022K/14339K, paused 1ms+1ms
12-20 20:49:02.507: INFO/dalvikvm(9247): Turning on JNI app bug workarounds for target SDK version 13...
12-20 20:49:02.507: INFO/ActivityManager(175): Start proc com.google.android.apps.maps:FriendService for broadcast com.google.android.apps.maps/com.google.googlenav.friend.androi
12-20 20:49:02.601: DEBUG/dalvikvm(9247): GC_CONCURRENT freed 153K, 2% free 14374K/14599K, paused 3ms+1ms
```


12-20 20:49:02.687: DEBUG/dalvikvm(9247): GC_CONCURRENT freed 134K, 2% free 14709K/14983K, paused 2ms+2ms
12-20 20:49:02.773: INFO/ActivityManager(175): Start proc com.google.android.googlequicksearchbox for broadcast com.google.android.googlequicksearchbox/.SourceUpdateReceiver: pic
12-20 20:49:02.781: DEBUG/dalvikvm(9247): GC_CONCURRENT freed 218K, 3% free 14925K/15239K, paused 1ms+3ms
12-20 20:49:02.804: INFO/ActivityThread(9260): Pub com.google.android.googlequicksearchbox.shortcuts: com.google.android.googlequicksearchbox.WebHistoryProvider
12-20 20:49:02.812: INFO/ActivityThread(9260): Pub com.google.android.googlequicksearchbox.google: com.google.android.googlequicksearchbox.google.GoogleSuggestionProvider
12-20 20:49:05.359: INFO/ActivityManager(175): Process com.google.android.gallery3d (pid 9219) has died.
12-20 20:49:05.382: DEBUG/dalvikvm(9169): GC_CONCURRENT freed 135K, 2% free 14375K/14599K, paused 3ms+1ms
12-20 20:49:05.437: DEBUG/dalvikvm(9169): GC_CONCURRENT freed 6K, 2% free 14809K/14983K, paused 3ms+5ms
12-20 20:49:09.828: INFO/WindowManager(175): createSurface Window{41b62f10 TrackingView paused=false}: DRAW NOW PENDING
12-20 20:49:09.921: INFO/ActivityManager(175): Process com.android.vending (pid 9118) has died.
12-20 20:49:10.468: DEBUG/OpenGLRenderer(315): Flushing caches (mode 0)
12-20 20:49:10.531: WARN/InputManagerService(175): Window already focused, ignoring focus gain of: com.android.internal.view.IInputMethodClient\$Stub\$Proxy@41a14240
12-20 20:49:12.429: DEBUG/MyAct(9169): On Pause() Called
12-20 20:49:12.445: INFO/WindowManager(175): createSurface Window{418802c8 com.android.launcher/com.android.launcher2.Launcher paused=false}: DRAW NOW PENDING
12-20 20:49:12.687: INFO/ActivityManager(175): Process com.google.android.partnersetup (pid 9232) has died.
12-20 20:49:12.726: WARN/InputManagerService(175): Starting input on non-focused client com.android.internal.view.IInputMethodClient\$Stub\$Proxy@41be0370 (uid=10059 pid=9169)
12-20 20:49:12.750: INFO/ActivityManager(175): Process com.google.android.apps.plus (pid 9154) has died.
12-20 20:49:13.320: DEBUG/MyAct(9169): On Destroy() called
12-20 20:49:24.296: DEBUG/dalvikvm(9169): GC_CONCURRENT freed 198K, 3% free 15042K/15367K, paused 2ms+4ms
12-20 20:49:24.718: DEBUG/dalvikvm(9169): GC_CONCURRENT freed 492K, 4% free 15005K/15623K, paused 1ms+4ms
12-20 20:49:25.070: DEBUG/dalvikvm(9169): GC_CONCURRENT freed 418K, 5% free 14981K/15623K, paused 1ms+4ms
12-20 20:49:25.429: DEBUG/dalvikvm(9169): GC_CONCURRENT freed 401K, 5% free 14975K/15623K, paused 1ms+4ms
12-20 20:49:25.914: DEBUG/dalvikvm(9169): GC_CONCURRENT freed 390K, 5% free 14969K/15623K, paused 2ms+4ms
12-20 20:49:39.968: INFO/ActivityManager(175): Process com.example (pid 9169) has died.

 **deleted**
0 B 

 **jb...@android.com** <jb...@android.com>
Status: Won't Fix (Obsolete)

 **ra...@gmail.com** <ra...@gmail.com> [#10](#)

I can confirm finding a very similar behavior in my app. My conclusions are that if you try to run javascript in the onActivityResult event all further javascript calls will not be made anymore ar file is chosen using a file picker.
Curiously enough, if I place a breakpoint before calling the js, in onActivityResult and then continue execution, everything works fine. I tried making the javascript call on a different thread usi

 **mo...@gmail.com** <mo...@gmail.com> [#11](#)

From issue 273883685 on 22.03.2023:

1. `androidx.window.extensions` is loaded dynamically. It is declared as a dependency using the `<uses-library>` tag <https://cs.android.com/androidx/platform/frameworks/support/+main>window/window/src/main/AndroidManifest.xml;drc=dcfa035a961fd1daabb7dccc97d77fa2a006abf;l=21>

What do you mean by "What are the rules for integrating this JAR file?" It is shipped on device.

2. It is up to the OEM to provide the `androidx.window.extensions.jar` and it should not be linked in any app. OEMs are required to include `androidx.window.extensions` for some de