

Forum:[Hack Forums](#)

Thread: [Android Task Hijacking](#)

source - September 9, 2022, 3:36 pm

Task, Back Stack and Foreground Activities

A task is a collection of activities that users interact with when performing a certain job. The activities are arranged in a stack—the back stack—in the order in which each activity is opened.

The activity that is displayed on the screen is called a foreground activity and its task is called the foreground task. At a time, only one foreground task is visible on the screen.

This is some simple activity flow:
There's only Activity 1 in the foreground.

Activity 2 is started which pushes Activity 1 to the Back Stack. Now Activity 2 is in the foreground.

Activity 3 is started which pushes both Activity 1 and 2 to the Back Stack.

Now when Activity 3 is closed. The previous activity i.e., 2 is brought automatically to the foreground. This is how task navigation works in Android.

Android Multi-tasking - One Task

One task is composed by several activities

Android Multi-tasking - Several Tasks

Android usually manages several tasks

Task Control Knobs

Task affinity attack

Task affinity and Launch Modes

Task affinity is an attribute that is defined in each <activity> tag in the AndroidManifest.xml file. It describes which Task an Activity prefers to join.

By default, every activity has the same affinity as the package name.

We'll be using this when creating our PoC app.

Code <activity android:taskAffinity=""/>

Launch modes allow you to define how a new instance of an activity is associated with the current task. The [launchMode](#) attribute specifies an instruction on how the activity should be launched into a task.

There are four different Launch Modes:

standard (Default)

singleTop

singleTask

singleInstance

When the launchMode is set to singleTask, the Android system evaluates three possibilities and one of them is the reason why our attack is possible. Here they are:

If the Activity instance already exists:

Android resumes the existing instance instead of creating a new one. It means that there is at most one activity instance in the system under this mode.

If creating a new activity instance is necessary:

The Activity Manager Service (AMS) selects a task to host the newly created instance by finding a “matching” one in all existing tasks. An activity “matches” a task if they have the same task affinity. This is the reason why we can specify the same task affinity as the vulnerable app in our malware/attacker's app so it launches in their task instead of creating it's own.

Without finding a “matching” task:

The AMS creates a new task and makes the new activity instance the root activity of the newly created task.

Attack

The victim needs to have the malicious app installed in his device. Then, he needs to open it before opening the vulnerable application. Then, when the vulnerable application is opened, the malicious application will be opened instead. If this malicious application presents the same login as the vulnerable application the user won't have any means to know that he is putting his credentials in a malicious application.

You can find an attack implemented here: https://github.com/az0mb13/Task_Hijacking_Strandhogg

Preventing task hijacking

Setting `taskAffinity=""` can be a quick fix for this issue. The launch mode can also be set to `singleInstance` if the app does not want other activities to join tasks belonging to it. A custom `onBackPressed()` function can also be added, to override the default behavior.

References

<https://blog.dixitaditya.com/android-task-hijacking/>

<https://blog.takemyhand.xyz/2021/02/android-task-hijacking-with.html>

source - October 5, 2022, 7:42 pm

(Oct 5, 2022 07:32 PM)Dyne Wrote: [\[CITE\]](#) Honestly, I'd like to see your search history.

FBI open up

EDIT: Honestly I love blogs like takemyhand

They are often very "no bullshit" here's what this does. Thank you for the share.

Takemyhand has taught me a lot

mickeh - October 5, 2022, 7:55 pm

(Oct 5, 2022 07:32 PM)Dyne Wrote: [\[CITE\]](#) Honestly, I'd like to see your search history.

FBI open up

EDIT: Honestly I love blogs like takemyhand

They are often very "no bullshit" here's what this does. Thank you for the share.

This actually made me laugh

Nice HQ post [source](#)