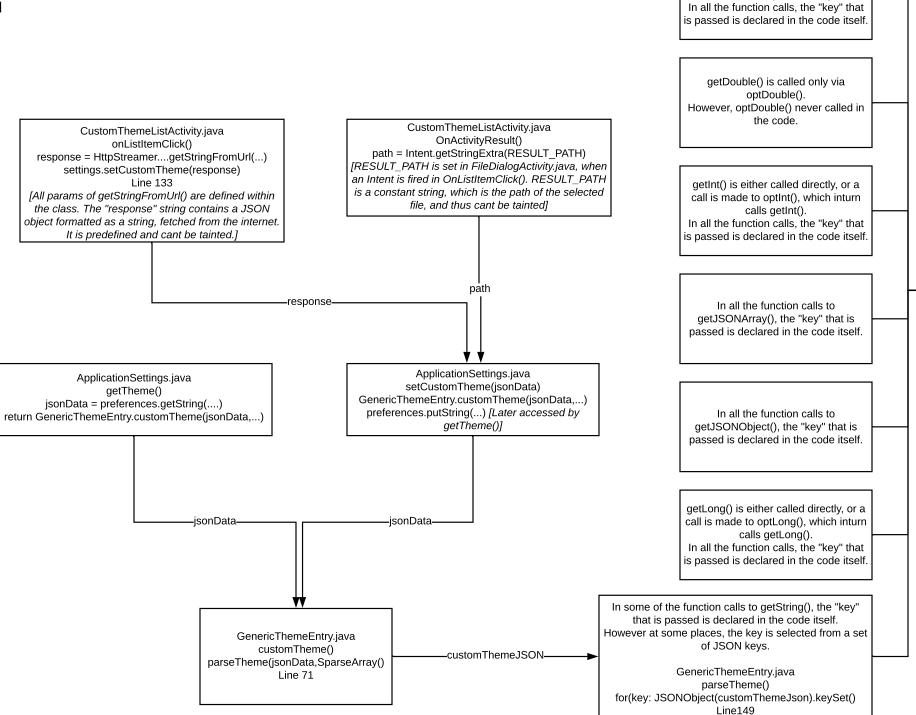1) Most of the parameters to the SINK are predefined
in the Code.
2) Some other parameters flow from outside the app,
from the Internet.
3) Thus, these parameters cant be tainted and the
flow is classified as FALSE POSITIVE

```
┌─────────────────────────────────────┐
│ CustomThemeListActivity.java         │
│ onListItemClick()                    │
│ response = HttpStreamer....getStringFromUrl(...) │
│ settings.setCustomTheme(response)    │
│ Line 133                             │
│ [All params of getStringFromUrl() are defined within │
│ the class. The "response" string contains a JSON │
│ object formatted as a string, fetched from the internet. │
│ It is predefined and cant be tainted.] │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ CustomThemeListActivity.java         │
│ OnActivityResult()                   │
│ path = Intent.getStringExtra(RESULT_PATH) │
│ [RESULT_PATH is set in FileDialogActivity.java, when │
│ an Intent is fired in OnListItemClick(). RESULT_PATH │
│ is a constant string, which is the path of the selected │
│ file, and thus cant be tainted] │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ getBoolean() is either called directly, or │
│ a call is made to optBoolean(), which │
│ inturn calls getBoolean().           │
│ In all the function calls, the "key" that │
│ is passed is declared in the code itself. │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ getDouble() is called only via       │
│ optDouble().                         │
│ However, optDouble() never called in │
│ the code.                            │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ getInt() is either called directly, or a │
│ call is made to optInt(), which inturn │
│ calls getInt().                      │
│ In all the function calls, the "key" that │
│ is passed is declared in the code itself. │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ In all the function calls to          │
│ getJSONArray(), the "key" that is     │
│ passed is declared in the code itself. │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ JSONObject.java                      │
│ get(key)                             │
│ getBoolean(key)                      │
│ geDouble(key)                        │
│ getInt(key)                          │
│ getJSONArray(key)                    │
│ getJSONObject(key)                   │
│ getLong(key)                         │
│ getString(key)                       │
│                                      │
│ throw new                            │
│ JSONEException(....quote(key)....)   │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ JSONObject.java                      │
│ quote()                              │
│ call to: quote(string, StringWriter) │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ SINK                                 │
│ JSONObject.java                      │
│ quote()                              │
│ Writer.write(int)                    │
│ Line 1244, 1250, 1275                │
│ [Ignoring other occurances of        │
│ Writer.write(int) as they take in a  │
│ constant char as a parameter]        │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ ApplicationSettings.java             │
│ getTheme()                           │
│ jsonData = preferences.getString(....) │
│ return GenericThemeEntry.customTheme(jsonData,...) │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ ApplicationSettings.java             │
│ setCustomTheme(jsonData)             │
│ GenericThemeEntry.customTheme(jsonData,...) │
│ preferences.putString(...) [Later accessed by │
│ getTheme()]                          │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ In all the function calls to          │
│ getJSONObject(), the "key" that is    │
│ passed is declared in the code itself. │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ getLong() is either called directly, or a │
│ call is made to optLong(), which inturn │
│ calls getLong().                     │
│ In all the function calls, the "key" that │
│ is passed is declared in the code itself. │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ GenericThemeEntry.java               │
│ customTheme()                        │
│ parseTheme(jsonData,SparseArray()    │
│ Line 71                              │
└─────────────────────────────────────┘
```

```
┌─────────────────────────────────────┐
│ In some of the function calls to getString(), the "key" │
│ that is passed is declared in the code itself. │
│ However at some places, the key is selected from a set │
│ of JSON keys.                        │
│                                      │
│ GenericThemeEntry.java               │
│ parseTheme()                         │
│ for(key: JSONObject(customThemeJson).keySet() │
│ Line149                              │
└─────────────────────────────────────┘
```

response
path
key
string
jsonData
jsonData
customThemeJSON