# CWE Detail – CWE-926

## Description

The Android application exports a component for use by other applications, but does not properly restrict which applications can launch the component or access the data it contains.

## Extended Description

The attacks and consequences of improperly exporting a component may depend on the exported component: If access to an exported Activity is not restricted, any application will be able to launch the activity. This may allow a malicious application to gain access to sensitive information, modify the internal state of the application, or trick a user into interacting with the victim application while believing they are still interacting with the malicious application. If access to an exported Service is not restricted, any application may start and bind to the Service. Depending on the exposed functionality, this may allow a malicious application to perform unauthorized actions, gain access to sensitive information, or corrupt the internal state of the application. If access to a Content Provider is not restricted to only the expected applications, then malicious applications might be able to access the sensitive data. Note that in Android before 4.2, the Content Provider is automatically exported unless it has been explicitly declared as NOT exported.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Unexpected State, DoS: Crash, Exit, or Restart, DoS: Instability, Varies by Context — Notes: Other applications, possibly untrusted, can launch the Activity.

**•** Impact: Unexpected State, Gain Privileges or Assume Identity, DoS: Crash, Exit, or Restart, DoS: Instability, Varies by Context — Notes: Other applications, possibly untrusted, can bind to the Service.

**•** Impact: Read Application Data, Modify Application Data — Notes: Other applications, possibly untrusted, can read or modify the data that is offered by the Content Provider.

## Potential Mitigations

**•** Build and Compilation: If they do not need to be shared by other applications, explicitly mark components with android:exported="false" in the application manifest. (Effectiveness: N/A)

**•** Build and Compilation: If you only intend to use exported components between related apps under your control, use android:protectionLevel="signature" in the xml manifest to restrict access to applications signed by you. (Effectiveness: N/A)

**•** Build and Compilation: Limit Content Provider permissions (read/write) as appropriate. (Effectiveness: N/A)

**•** Build and Compilation: Limit Content Provider permissions (read/write) as appropriate. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** Because these components have intent filters but have not explicitly set 'android:exported=false' elsewhere in the manifest, they are automatically exported so that any other application can launch them. This may lead to unintended behavior or exploits.

**•** Because this content provider is only intended to be used within the application, it does not need to be exported. However, in Android before 4.2, it is automatically exported thus potentially allowing malicious applications to access sensitive information.