# CWE Detail – CWE-927

## Description

The Android application uses an implicit intent for transmitting sensitive data to other applications.

## Extended Description

Since an implicit intent does not specify a particular application to receive the data, any application can process the intent by using an Intent Filter for that intent. This can allow untrusted applications to obtain sensitive data. There are two variations on the standard broadcast intent, ordered and sticky. Ordered broadcast intents are delivered to a series of registered receivers in order of priority as declared by the Receivers. A malicious receiver can give itself a high priority and cause a denial of service by stopping the broadcast from propagating further down the chain. There is also the possibility of malicious data modification, as a receiver may also alter the data within the Intent before passing it on to the next receiver. The downstream components have no way of asserting that the data has not been altered earlier in the chain. Sticky broadcast intents remain accessible after the initial broadcast. An old sticky intent will be broadcast again to any new receivers that register for it in the future, greatly increasing the chances of information exposure over time. Also, sticky broadcasts cannot be protected by permissions that may apply to other kinds of intents. In addition, any broadcast intent may include a URI that references data that the receiving component does not normally have the privileges to access. The sender of the intent can include special privileges that grant the receiver read or write access to the specific URI included in the intent. A malicious receiver that intercepts this intent will also gain those privileges and be able to read or write the resource at the specified URI.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Observed Examples (CVEs)

**•** CVE-2022-4903: An Android application does not use FLAG\_IMMUTABLE when creating a PendingIntent.

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: Other applications, possibly untrusted, can read the data that is offered through the Intent.

**•** Impact: Varies by Context — Notes: The application may handle responses from untrusted applications on the device, which could cause it to perform unexpected or unauthorized actions.

## Potential Mitigations

**•** Implementation: If the application only requires communication with its own components, then the destination is always known, and an explicit intent could be used. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** This application assumes only the trusted applications will be listening for the action. A malicious application can register for this action and intercept the user's login information, as below:

**•** Sticky broadcasts can be read by any application at any time, and so should never contain sensitive information such as a username.

**•** Any application in the broadcast chain may alter the data within the intent. This malicious application is altering the URL to point to an attack site:

**•** Any malicious application can register to receive this intent. Because of the FLAG\_GRANT\_READ\_URI\_PERMISSION included with the intent, the malicious receiver code can read the user's data.