# CWE Detail – CWE-925

## Description

The Android application uses a Broadcast Receiver that receives an Intent but does not properly verify that the Intent came from an authorized source.

## Extended Description

Certain types of Intents, identified by action string, can only be broadcast by the operating system itself, not by third-party applications. However, when an application registers to receive these implicit system intents, it is also registered to receive any explicit intents. While a malicious application cannot send an implicit system intent, it can send an explicit intent to the target application, which may assume that any received intent is a valid implicit system intent and not an explicit intent from another application. This may lead to unintended behavior.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-499

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes: Another application can impersonate the operating system and cause the software to perform an unintended action.

## Potential Mitigations

**•** Architecture and Design: Before acting on the Intent, check the Intent Action to make sure it matches the expected System action. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The ShutdownReceiver class will handle the intent:

## Notes

**•** Maintenance: This entry will be made more comprehensive in later CWE versions.