# CWE Detail – CWE-921

## Description

The product stores sensitive information in a file system or device that does not have built-in access control.

## Extended Description

While many modern file systems or devices utilize some form of access control in order to restrict access to data, not all storage mechanisms have this capability. For example, memory cards, floppy disks, CDs, and USB devices are typically made accessible to any user within the system. This can become a problem when sensitive data is stored in these mechanisms in a multi-user environment, because anybody on the system can read or write this data. On Android devices, external storage is typically globally readable and writable by other applications on the device. External storage may also be easily accessible through the mobile device's USB connection or physically accessible through the device's memory card port.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Modes of Introduction

**•** Architecture and Design: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

## Common Consequences

**•** Impact: Read Application Data, Read Files or Directories — Notes: Attackers can read sensitive information by accessing the unrestricted storage mechanism.

**•** Impact: Modify Application Data, Modify Files or Directories — Notes: Attackers can modify or delete sensitive information by accessing the unrestricted storage mechanism.

## Applicable Platforms

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