# CWE Detail – CWE-266

## Description

A product incorrectly assigns a privilege to a particular actor, creating an unintended sphere of control for that actor.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-1999-1193: untrusted user placed in unix "wheel" group

**•** CVE-2005-2741: Product allows users to grant themselves certain rights that can be used to escalate privileges.

**•** CVE-2005-2496: Product uses group ID of a user instead of the group, causing it to run with different privileges. This is resultant from some other unknown issue.

**•** CVE-2004-0274: Product mistakenly assigns a particular status to an entity, leading to increased privileges.

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes: A user can access restricted functionality and/or sensitive information that may include administrative functionality and user accounts.

## Potential Mitigations

**•** Architecture and Design: Very carefully manage the setting, management, and handling of privileges. Explicitly manage trust zones in the software. (Effectiveness: N/A)

**•** Architecture and Design: Run your code using the lowest privileges that are required to accomplish the necessary tasks [REF-76]. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

**•** N/A

**•** 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.