# CWE Detail – CWE-268

## Description

Two distinct privileges, roles, capabilities, or rights can be combined in a way that allows an entity to perform unsafe actions that would not be allowed without that combination.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2005-1736: Chaining of user rights.

**•** CVE-2002-1772: Gain certain rights via privilege chaining in alternate channel.

**•** CVE-2005-1973: Application is allowed to assign extra permissions to itself.

**•** CVE-2003-0640: "operator" user can overwrite usernames and passwords to gain admin privileges.

## Modes of Introduction

**•** Architecture and Design: N/A

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

**•** Operation: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes: A user can be given or gain access rights of another user. This can give the user unauthorized access to sensitive information including the access information of another user.

## Potential Mitigations

**•** Architecture and Design: Consider following the principle of separation of privilege. Require multiple conditions to be met before permitting access to a system resource. (Effectiveness: N/A)

**•** 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

**•** This code does not check the role of the user whose password is being reset. It is possible for an Operator to gain Admin privileges by resetting the password of an Admin account and taking control of that account.

## Notes

**•** Relationship: There is some conceptual overlap with Unsafe Privilege.