# CWE Detail – CWE-283

## Description

The product does not properly verify that a critical resource is owned by the proper entity.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2001-0178: Program does not verify the owner of a UNIX socket that is used for sending a password.

**•** CVE-2004-2012: Owner of special device not checked, allowing root.

## Modes of Introduction

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

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes: An attacker could gain unauthorized access to system resources.

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

## Applicable Platforms

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

## Demonstrative Examples

**•** This code does not confirm that the process to be killed is owned by the requesting user, thus allowing an attacker to kill arbitrary processes.

## Notes

**•** Relationship: This overlaps insufficient comparison, verification errors, permissions, and privileges.