# CWE Detail – CWE-274

## Description

The product does not handle or incorrectly handles when it has insufficient privileges to perform an operation, leading to resultant weaknesses.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2001-1564: System limits are not properly enforced after privileges are dropped.

**•** CVE-2005-3286: Firewall crashes when it can't read a critical memory block that was protected by a malicious process.

**•** CVE-2005-1641: Does not give admin sufficient privileges to overcome otherwise legitimate user actions.

## Modes of Introduction

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

**•** Operation: N/A

## Common Consequences

**•** Impact: Other, Alter Execution Logic — Notes:

## Applicable Platforms

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

## Notes

**•** Maintenance: CWE-280 and CWE-274 are too similar. It is likely that CWE-274 will be deprecated in the future.

**•** Relationship: Overlaps dropped privileges, insufficient permissions.

**•** Theoretical: This has a layering relationship with Unchecked Error Condition and Unchecked Return Value.

**•** Theoretical: Within the context of vulnerability theory, privileges and permissions are two sides of the same coin. Privileges are associated with actors, and permissions are associated with resources. To perform access control, at some point the product makes a decision about whether the actor (and the privileges that have been assigned to that actor) is allowed to access the resource (based on the permissions that have been specified for that resource).