# CWE Detail – CWE-269

## Description

The product does not properly assign, modify, track, or check privileges for an 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-2001-1555: Terminal privileges are not reset when a user logs out.

**•** CVE-2001-1514: Does not properly pass security context to child processes in certain cases, allows privilege escalation.

**•** CVE-2001-0128: Does not properly compute roles.

**•** 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.

**•** CVE-2007-4217: FTP client program on a certain OS runs with setuid privileges and has a buffer overflow. Most clients do not need extra privileges, so an overflow is not a vulnerability for those clients.

**•** CVE-2007-5159: OS incorrectly installs a program with setuid privileges, allowing users to gain privileges.

**•** CVE-2008-4638: Composite: application running with high privileges (CWE-250) allows user to specify a restricted file to process, which generates a parsing error that leaks the contents of the file (CWE-209).

**•** CVE-2007-3931: Installation script installs some programs as setuid when they shouldn't be.

**•** CVE-2002-1981: Roles have access to dangerous procedures (Accessible entities).

**•** CVE-2002-1671: Untrusted object/method gets access to clipboard (Accessible entities).

**•** CVE-2000-0315: Traceroute program allows unprivileged users to modify source address of packet (Accessible entities).

**•** CVE-2000-0506: User with capability can prevent setuid program from dropping privileges (Unsafe privileged actions).

## Related Attack Patterns (CAPEC)

* CAPEC-122
* CAPEC-233
* CAPEC-58

## Attack TTPs

**•** T1548: Abuse Elevation Control Mechanism (Tactics: privilege-escalation, defense-evasion)

## 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:

## 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: Follow the principle of least privilege when assigning access rights to entities in a software system. (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

**•** While the program only raises its privilege level to create the folder and immediately lowers it again, if the call to os.mkdir() throws an exception, the call to lowerPrivileges() will not occur. As a result, the program is indefinitely operating in a raised privilege state, possibly allowing further exploitation to occur.

**•** N/A

**•** N/A

**•** While the intention was to only allow Administrators to print the debug information, the code as written only excludes those with the role of "GUEST". Someone with the role of "ADMIN" or "USER" will be allowed access, which goes against the original intent. An attacker may be able to use this debug information to craft an attack on the system.

**•** 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

**•** Maintenance: The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-693).