# CWE Detail – CWE-267

## Description

A particular privilege, role, capability, or right can be used to perform unsafe actions that were not intended, even when it is assigned to the correct entity.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

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

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

**•** CVE-2004-2204: Gain privileges using functions/tags that should be restricted (Accessible entities).

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

**•** CVE-2004-0380: Bypass domain restrictions using a particular file that references unsafe URI schemes (Accessible entities).

**•** CVE-2002-1154: Script does not restrict access to an update command, leading to resultant disk consumption and filled error logs (Accessible entities).

**•** CVE-2002-1145: "public" database user can use stored procedure to modify data controlled by the database owner (Unsafe privileged actions).

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

**•** CVE-2002-2042: Allows attachment to and modification of privileged processes (Unsafe privileged actions).

**•** CVE-2000-1212: User with privilege can edit raw underlying object using unprotected method (Unsafe privileged actions).

**•** CVE-2005-1742: Inappropriate actions allowed by a particular role(Unsafe privileged actions).

**•** CVE-2001-1480: Untrusted entity allowed to access the system clipboard (Unsafe privileged actions).

**•** CVE-2001-1551: Extra Linux capability allows bypass of system-specified restriction (Unsafe privileged actions).

**•** CVE-2001-1166: User with debugging rights can read entire process (Unsafe privileged actions).

**•** CVE-2005-1816: Non-root admins can add themselves or others to the root admin group (Unsafe privileged actions).

**•** CVE-2005-2173: Users can change certain properties of objects to perform otherwise unauthorized actions (Unsafe privileged actions).

**•** CVE-2005-2027: Certain debugging commands not restricted to just the administrator, allowing registry modification and infoleak (Unsafe privileged actions).

## Related Attack Patterns (CAPEC)

* CAPEC-58
* CAPEC-634
* CAPEC-637
* CAPEC-643
* CAPEC-648

## Attack TTPs

**•** T1113: Screen Capture (Tactics: collection)

**•** T1123: Audio Capture (Tactics: collection)

**•** T1115: Clipboard Data (Tactics: collection)

**•** T1135: Network Share Discovery (Tactics: discovery)

**•** T1125: Video Capture (Tactics: collection)

## 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 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

**•** 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.

## Notes

**•** Maintenance: Note: there are 2 separate sub-categories here: - privilege incorrectly allows entities to perform certain actions - object is incorrectly accessible to entities with a given privilege