# CWE Detail – CWE-708

## Description

The product assigns an owner to a resource, but the owner is outside of the intended control sphere.

## Extended Description

This may allow the resource to be manipulated by actors outside of the intended control sphere.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2007-5101: File system sets wrong ownership and group when creating a new file.

**•** CVE-2007-4238: OS installs program with bin owner/group, allowing modification.

**•** CVE-2007-1716: Manager does not properly restore ownership of a reusable resource when a user logs out, allowing privilege escalation.

**•** CVE-2005-3148: Backup software restores symbolic links with incorrect uid/gid.

**•** CVE-2005-1064: Product changes the ownership of files that a symlink points to, instead of the symlink itself.

**•** CVE-2011-1551: Component assigns ownership of sensitive directory tree to a user account, which can be leveraged to perform privileged operations.

## 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: Read Application Data, Modify Application Data — Notes: An attacker could read and modify data for which they do not have permissions to access directly.

## Potential Mitigations

**•** Policy: Periodically review the privileges and their owners. (Effectiveness: N/A)

**•** Testing: Use automated tools to check for privilege settings. (Effectiveness: N/A)

## Applicable Platforms

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

## Notes

**•** Maintenance: This overlaps verification errors, permissions, and privileges. A closely related weakness is the incorrect assignment of groups to a resource. It is not clear whether it would fall under this entry or require a different entry.