# CWE Detail – CWE-668

## Description

The product exposes a resource to the wrong control sphere, providing unintended actors with inappropriate access to the resource.

## Extended Description

Resources such as files and directories may be inadvertently exposed through mechanisms such as insecure permissions, or when a program accidentally operates on the wrong object. For example, a program may intend that private files can only be provided to a specific user. This effectively defines a control sphere that is intended to prevent attackers from accessing these private files. If the file permissions are insecure, then parties other than the user will be able to access those files. A separate control sphere might effectively require that the user can only access the private files, but not any other files on the system. If the program does not ensure that the user is only requesting private files, then the user might be able to access other files on the system. In either case, the end result is that a resource has been exposed to the wrong party.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## 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 — Notes: An adversary that gains access to a resource exposed to a wrong sphere could potentially retrieve private data from that resource, thus breaking the intended confidentiality of that data.

**•** Impact: Modify Application Data — Notes: An adversary that gains access to a resource exposed to a wrong sphere could potentially modify data held within that resource, thus breaking the intended integrity of that data and causing the system relying on that resource to make unintended decisions.

**•** Impact: Varies by Context — Notes: The consequences may vary widely depending on how the product uses the affected resource.

## Notes

**•** Theoretical: A "control sphere" is a set of resources and behaviors that are accessible to a single actor, or a group of actors. A product's security model will typically define multiple spheres, possibly implicitly. For example, a server might define one sphere for "administrators" who can create new user accounts with subdirectories under /home/server/, and a second sphere might cover the set of users who can create or delete files within their own subdirectories. A third sphere might be "users who are authenticated to the operating system on which the product is installed." Each sphere has different sets of actors and allowable behaviors.