# CWE Detail – CWE-529

## Description

The product stores access control list files in a directory or other container that is accessible to actors outside of the intended control sphere.

## Extended Description

Exposure of these access control list files may give the attacker information about the configuration of the site or system. This information may then be used to bypass the intended security policy or identify trusted systems from which an attack can be launched.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Operation: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

## Common Consequences

**•** Impact: Read Application Data, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** System Configuration: Protect access control list files. (Effectiveness: N/A)