# CWE Detail – CWE-279

## Description

While it is executing, the product sets the permissions of an object in a way that violates the intended permissions that have been specified by the user.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-0265: Log files opened read/write.

**•** CVE-2003-0876: Log files opened read/write.

**•** CVE-2002-1694: Log files opened read/write.

## Related Attack Patterns (CAPEC)

* CAPEC-81

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

**•** Architecture and Design: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data, Modify Application Data — 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: Compartmentalize the system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area. Ensure that appropriate compartmentalization is built into the system design, and the compartmentalization allows for and reinforces privilege separation functionality. Architects and designers should rely on the principle of least privilege to decide the appropriate time to use privileges and the time to drop privileges. (Effectiveness: N/A)

## Applicable Platforms

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