# CWE Detail – CWE-455

## Description

The product does not exit or otherwise modify its operation when security-relevant errors occur during initialization, such as when a configuration file has a format error or a hardware security module (HSM) cannot be activated, which can cause the product to execute in a less secure fashion than intended by the administrator.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2005-1345: Product does not trigger a fatal error if missing or invalid ACLs are in a configuration file.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Application Data, Alter Execution Logic — Notes: The application could be placed in an insecure state that may allow an attacker to modify sensitive data or allow unintended logic to be executed.

## Potential Mitigations

**•** Implementation: Follow the principle of failing securely when an error occurs. The system should enter a state where it is not vulnerable and will not display sensitive error messages to a potential attacker. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** If the application is unable to extract the state information - say, due to a database timeout - then the $uid variable will not be explicitly set by the programmer. This will cause $uid to be regarded as equivalent to "0" in the conditional, allowing the original user to perform administrator actions. Even if the attacker cannot directly influence the state data, unexpected errors could cause incorrect privileges to be assigned to a user just by accident.

## Notes

**•** Research Gap: Under-studied. These issues are not frequently reported, and it is difficult to find published examples.