# CWE Detail – CWE-372

## Description

The product does not properly determine which state it is in, causing it to assume it is in state X when in fact it is in state Y, causing it to perform incorrect operations in a security-relevant manner.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-140
* CAPEC-74

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context, Unexpected State — Notes:

## Applicable Platforms

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

## Notes

**•** Relationship: This conceptually overlaps other categories such as insufficient verification, but this entry refers to the product's incorrect perception of its own state.

**•** Relationship: This is probably resultant from other weaknesses such as unhandled error conditions, inability to handle out-of-order steps, multiple interpretation errors, etc.

**•** Maintenance: This entry is being considered for deprecation. It was poorly-defined in PLOVER and is not easily described using the behavior/resource/property model of vulnerability theory.