# CWE Detail – CWE-386

## Description

A constant symbolic reference to an object is used, even though the reference can resolve to a different object over time.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes: The attacker can gain access to otherwise unauthorized resources.

**•** Impact: Modify Application Data, Modify Files or Directories, Read Application Data, Read Files or Directories, Other — Notes: Race conditions such as this kind may be employed to gain read or write access to resources not normally readable or writable by the user in question.

**•** Impact: Modify Application Data, Other — Notes: The resource in question, or other resources (through the corrupted one) may be changed in undesirable ways by a malicious user.

**•** Impact: Hide Activities — Notes: If a file or other resource is written in this method, as opposed to a valid way, logging of the activity may not occur.

**•** Impact: Modify Files or Directories — Notes: In some cases it may be possible to delete files that a malicious user might not otherwise have access to -- such as log files.

## Applicable Platforms

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