# CWE Detail – CWE-666

## Description

The product performs an operation on a resource at the wrong phase of the resource's lifecycle, which can lead to unexpected behaviors.

## Extended Description

A resource's lifecycle includes several phases: initialization, use, and release. For each phase, it is important to follow the specifications outlined for how to operate on the resource and to ensure that the resource is in the expected phase. Otherwise, if a resource is in one phase but the operation is not valid for that phase (i.e., an incorrect phase of the resource's lifetime), then this can produce resultant weaknesses. For example, using a resource before it has been fully initialized could cause corruption or incorrect data to be used.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2006-5051: Chain: Signal handler contains too much functionality (CWE-828), introducing a race condition (CWE-362) that leads to a double free (CWE-415).

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Other — Notes:

## Potential Mitigations

**•** Architecture and Design: Follow the resource's lifecycle from creation to release. (Effectiveness: N/A)

## Demonstrative Examples

**•** Double free vulnerabilities have two common (and sometimes overlapping) causes: