# CWE Detail – CWE-663

## Description

The product calls a non-reentrant function in a concurrent context in which a competing code sequence (e.g. thread or signal handler) may have an opportunity to call the same function or otherwise influence its state.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2001-1349: unsafe calls to library functions from signal handler

**•** CVE-2004-2259: SIGCHLD signal to FTP server can cause crash under heavy load while executing non-reentrant functions like malloc/free.

## Related Attack Patterns (CAPEC)

* CAPEC-29

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Memory, Read Memory, Modify Application Data, Read Application Data, Alter Execution Logic — Notes:

## Potential Mitigations

**•** Implementation: Use reentrant functions if available. (Effectiveness: N/A)

**•** Implementation: Add synchronization to your non-reentrant function. (Effectiveness: N/A)

**•** Implementation: In Java, use the ReentrantLock Class. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A

**•** N/A