# CWE Detail – CWE-394

## Description

The product does not properly check when a function or operation returns a value that is legitimate for the function, but is not expected by the product.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2004-1395: Certain packets (zero byte and other lengths) cause a recvfrom call to produce an unexpected return code that causes a server's listening loop to exit.

**•** CVE-2002-2124: Unchecked return code from recv() leads to infinite loop.

**•** CVE-2005-2553: Kernel function does not properly handle when a null is returned by a function call, causing it to call another function that it shouldn't.

**•** CVE-2005-1858: Memory not properly cleared when read() function call returns fewer bytes than expected.

**•** CVE-2000-0536: Bypass access restrictions when connecting from IP whose DNS reverse lookup does not return a hostname.

**•** CVE-2001-0910: Bypass access restrictions when connecting from IP whose DNS reverse lookup does not return a hostname.

**•** CVE-2004-2371: Game server doesn't check return values for functions that handle text strings and associated size values.

**•** CVE-2005-1267: Resultant infinite loop when function call returns -1 value.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Unexpected State, Alter Execution Logic — Notes:

## Applicable Platforms

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

## Notes

**•** Relationship: Usually primary, but can be resultant from issues such as behavioral change or API abuse. This can produce resultant vulnerabilities.