# CWE Detail – CWE-369

## Description

The product divides a value by zero.

## Extended Description

This weakness typically occurs when an unexpected value is provided to the product, or if an error occurs that is not properly detected. It frequently occurs in calculations involving physical dimensions such as size, length, width, and height.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2007-3268: Invalid size value leads to divide by zero.

**•** CVE-2007-2723: "Empty" content triggers divide by zero.

**•** CVE-2007-2237: Height value of 0 triggers divide by zero.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart — Notes: A Divide by Zero results in a crash.

## Demonstrative Examples

**•** By validating the input value used as the denominator the following code will ensure that a divide by zero error will not cause unexpected results. The following Java code example will validate the input value, output an error message, and throw an exception.

**•** By validating the input value used as the denominator the following code will ensure that a divide by zero error will not cause unexpected results. If the method is called and a zero is passed as the second argument a DivideByZero error will be thrown and should be caught by the calling block with an output message indicating the error.

**•** The method can be modified to raise, catch and handle the DivideByZeroException if the input value used as the denominator is zero.