# CWE Detail – CWE-683

## Description

The product calls a function, procedure, or routine, but the caller specifies the arguments in an incorrect order, leading to resultant weaknesses.

## Extended Description

While this weakness might be caught by the compiler in some languages, it can occur more frequently in cases in which the called function accepts variable numbers or types of arguments, such as format strings in C. It also can occur in languages or environments that do not enforce strong typing.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2006-7049: Application calls functions with arguments in the wrong order, allowing attacker to bypass intended access restrictions.

## Modes of Introduction

**•** Implementation: This problem typically occurs when the programmer makes a typo, or copy and paste errors.

## Common Consequences

**•** Impact: Quality Degradation — Notes:

## Potential Mitigations

**•** Implementation: Use the function, procedure, or routine as specified. (Effectiveness: N/A)

**•** Testing: Because this function call often produces incorrect behavior it will usually be detected during testing or normal operation of the product. During testing exercise all possible control paths will typically expose this weakness except in rare cases when the incorrect function call accidentally produces the correct results or if the provided argument type is very similar to the expected argument type. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A