# CWE Detail – CWE-628

## Description

The product calls a function, procedure, or routine with arguments that are not correctly specified, leading to always-incorrect behavior and resultant weaknesses.

## Extended Description

There are multiple ways in which this weakness can be introduced, including: the wrong variable or reference; an incorrect number of arguments; incorrect order of arguments; wrong type of arguments; or wrong value.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2006-7049: The method calls the functions with the wrong argument order, which allows remote attackers to bypass intended access restrictions.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Quality Degradation, Gain Privileges or Assume Identity — Notes: This weakness can cause unintended behavior and can lead to additional weaknesses such as allowing an attacker to gain unintended access to system resources.

## Potential Mitigations

**•** Build and Compilation: Once found, these issues are easy to fix. Use code inspection tools and relevant compiler features to identify potential violations. Pay special attention to code that is not likely to be exercised heavily during QA. (Effectiveness: N/A)

**•** Architecture and Design: Make sure your API's are stable before you use them in production code. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

**•** N/A

**•** N/A