# CWE Detail – CWE-393

## Description

A function or operation returns an incorrect return value or status code that does not indicate the true result of execution, causing the product to modify its behavior based on the incorrect result.

## Extended Description

This can lead to unpredictable behavior. If the function is used to make security-critical decisions or provide security-critical information, then the wrong status code can cause the product to assume that an action is safe or correct, even when it is not.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2003-1132: DNS server returns wrong response code for non-existent AAAA record, which effectively says that the domain is inaccessible.

**•** CVE-2001-1509: Hardware-specific implementation of system call causes incorrect results from geteuid.

**•** CVE-2001-1559: Chain: System call returns wrong value (CWE-393), leading to a resultant NULL dereference (CWE-476).

**•** CVE-2014-1266: chain: incorrect "goto" in Apple SSL product bypasses certificate validation, allowing Adversary-in-the-Middle (AITM) attack (Apple "goto fail" bug). CWE-705 (Incorrect Control Flow Scoping) -> CWE-561 (Dead Code) -> CWE-295 (Improper Certificate Validation) -> CWE-393 (Return of Wrong Status Code) -> CWE-300 (Channel Accessible by Non-Endpoint).

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Unexpected State, Alter Execution Logic — Notes: This weakness could place the system in a state that could lead unexpected logic to be executed or other unintended behaviors.

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

## Notes

**•** Relationship: This can be primary or resultant, but it is probably most often primary to other issues.