# CWE Detail – CWE-392

## Description

The product encounters an error but does not provide a status code or return value to indicate that an error has occurred.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** [REF-1374]: Chain: JavaScript-based cryptocurrency library can fall back to the insecure Math.random() function instead of reporting a failure (CWE-392), thus reducing the entropy (CWE-332) and leading to generation of non-unique cryptographic keys for Bitcoin wallets (CWE-1391)

**•** CVE-2004-0063: Function returns "OK" even if another function returns a different status code than expected, leading to accepting an invalid PIN number.

**•** CVE-2002-1446: Error checking routine in PKCS#11 library returns "OK" status even when invalid signature is detected, allowing spoofed messages.

**•** CVE-2002-0499: Kernel function truncates long pathnames without generating an error, leading to operation on wrong directory.

**•** CVE-2005-2459: Function returns non-error value when a particular erroneous condition is encountered, leading to resultant NULL dereference.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context, Unexpected State — Notes: Errors that are not properly reported could place the system in an unexpected state that could lead to unintended behaviors.

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A