# CWE Detail – CWE-684

## Description

The code does not function according to its published specifications, potentially leading to incorrect usage.

## Extended Description

When providing functionality to an external party, it is important that the product behaves in accordance with the details specified. When requirements of nuances are not documented, the functionality may produce unintended behaviors for the caller, possibly leading to an exploitable state.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

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

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

**•** CVE-2003-0187: Program uses large timeouts on unconfirmed connections resulting from inconsistency in linked lists implementations.

**•** CVE-1999-1446: UI inconsistency; visited URLs list not cleared when "Clear History" option is selected.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Implementation: Ensure that your code strictly conforms to specifications. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A

**•** N/A