# CWE Detail – CWE-758

## Description

The product uses an API function, data structure, or other entity in a way that relies on properties that are not always guaranteed to hold for that entity.

## Extended Description

This can lead to resultant weaknesses when the required properties change, such as when the product is ported to a different platform or if an interaction error (CWE-435) occurs.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2006-1902: Change in C compiler behavior causes resultant buffer overflows in programs that depend on behaviors that were undefined in the C standard.

## Common Consequences

**•** Impact: Other — Notes:

## Demonstrative Examples

**•** The same function may not always be found at the same memory address. This could lead to a crash, or an attacker may alter the memory at the expected address, leading to arbitrary code execution.

**•** N/A