# CWE Detail – CWE-188

## Description

The product makes invalid assumptions about how protocol data or memory is organized at a lower level, resulting in unintended program behavior.

## Extended Description

When changing platforms or protocol versions, in-memory organization of data may change in unintended ways. For example, some architectures may place local variables A and B right next to each other with A on top; some may place them next to each other with B on top; and others may add some padding to each. The padding size may vary to ensure that each variable is aligned to a proper word size. In protocol implementations, it is common to calculate an offset relative to another field to pick out a specific piece of data. Exceptional conditions, often involving new protocol versions, may add corner cases that change the data layout in an unusual way. The result can be that an implementation accesses an unintended field in the packet, treating data of one type as data of another type.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Memory, Read Memory — Notes: Can result in unintended modifications or exposure of sensitive memory.

## Potential Mitigations

**•** Implementation: In flat address space situations, never allow computing memory addresses as offsets from another memory address. (Effectiveness: N/A)

**•** Architecture and Design: Fully specify protocol layout unambiguously, providing a structured grammar (e.g., a compilable yacc grammar). (Effectiveness: N/A)

**•** Testing: Testing: Test that the implementation properly handles each case in the protocol grammar. (Effectiveness: N/A)

## Applicable Platforms

**•** C (Class: None, Prevalence: Undetermined)

**•** C++ (Class: None, Prevalence: Undetermined)

## Demonstrative Examples

**•** Here, b may not be one byte past a. It may be one byte in front of a. Or, they may have three bytes between them because they are aligned on 32-bit boundaries.