# CWE Detail – CWE-786

## Description

The product reads or writes to a buffer using an index or pointer that references a memory location prior to the beginning of the buffer.

## Extended Description

This typically occurs when a pointer or its index is decremented to a position before the buffer, when pointer arithmetic results in a position before the beginning of the valid memory location, or when a negative index is used.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-2227: Unchecked length of SSLv2 challenge value leads to buffer underflow.

**•** CVE-2007-4580: Buffer underflow from a small size value with a large buffer (length parameter inconsistency, CWE-130)

**•** CVE-2007-1584: Buffer underflow from an all-whitespace string, which causes a counter to be decremented before the buffer while looking for a non-whitespace character.

**•** CVE-2007-0886: Buffer underflow resultant from encoded data that triggers an integer overflow.

**•** CVE-2006-6171: Product sets an incorrect buffer size limit, leading to "off-by-two" buffer underflow.

**•** CVE-2006-4024: Negative value is used in a memcpy() operation, leading to buffer underflow.

**•** CVE-2004-2620: Buffer underflow due to mishandled special characters

## Common Consequences

**•** Impact: Read Memory — Notes: For an out-of-bounds read, the attacker may have access to sensitive information. If the sensitive information contains system details, such as the current buffer's position in memory, this knowledge can be used to craft further attacks, possibly with more severe consequences.

**•** Impact: Modify Memory, DoS: Crash, Exit, or Restart — Notes: Out of bounds memory access will very likely result in the corruption of relevant memory, and perhaps instructions, possibly leading to a crash.

**•** Impact: Modify Memory, Execute Unauthorized Code or Commands — Notes: If the corrupted memory can be effectively controlled, it may be possible to execute arbitrary code. If the corrupted memory is data rather than instructions, the system will continue to function with improper changes, possibly in violation of an implicit or explicit policy.

## Applicable Platforms

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

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

## Demonstrative Examples

**•** However, this function can cause a buffer underwrite if the input character string contains all whitespace. On some systems the while statement will move backwards past the beginning of a character string and will call the isspace() function on an address outside of the bounds of the local buffer.

**•** The programmer allows the user to specify which element in the list to select, however an attacker can provide an out-of-bounds offset, resulting in a buffer over-read (CWE-126).

**•** In the case where the substring is not found in destBuf, strstr() will return NULL, causing the pointer arithmetic to be undefined, potentially setting the value of idx to a negative number. If idx is negative, this will result in a buffer underwrite of destBuf.