# CWE Detail – CWE-196

## Description

The product uses an unsigned primitive and performs a cast to a signed primitive, which can produce an unexpected value if the value of the unsigned primitive can not be represented using a signed primitive.

## Extended Description

Although less frequent an issue than signed-to-unsigned conversion, unsigned-to-signed conversion can be the perfect precursor to dangerous buffer underwrite conditions that allow attackers to move down the stack where they otherwise might not have access in a normal buffer overflow condition. Buffer underwrites occur frequently when large unsigned values are cast to signed values, and then used as indexes into a buffer or for pointer arithmetic.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-92

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart — Notes: Incorrect sign conversions generally lead to undefined behavior, and therefore crashes.

**•** Impact: Modify Memory — Notes: If a poor cast lead to a buffer overflow or similar condition, data integrity may be affected.

**•** Impact: Execute Unauthorized Code or Commands, Bypass Protection Mechanism — Notes: Improper signed-to-unsigned conversions without proper checking can sometimes trigger buffer overflows which can be used to execute arbitrary code. This is usually outside the scope of a program's implicit security policy.

## Potential Mitigations

**•** Requirements: Choose a language which is not subject to these casting flaws. (Effectiveness: N/A)

**•** Architecture and Design: Design object accessor functions to implicitly check values for valid sizes. Ensure that all functions which will be used as a size are checked previous to use as a size. If the language permits, throw exceptions rather than using in-band errors. (Effectiveness: N/A)

**•** Implementation: Error check the return values of all functions. Be aware of implicit casts made, and use unsigned variables for sizes if at all possible. (Effectiveness: N/A)

## Applicable Platforms

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

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