# CWE Detail – CWE-128

## Description

Wrap around errors occur whenever a value is incremented past the maximum value for its type and therefore "wraps around" to a very small, negative, or undefined value.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-92

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart, DoS: Resource Consumption (CPU), DoS: Resource Consumption (Memory), DoS: Instability — Notes: This weakness will generally lead to undefined behavior and therefore crashes. In the case of overflows involving loop index variables, the likelihood of infinite loops is also high.

**•** Impact: Modify Memory — Notes: If the value in question is important to data (as opposed to flow), simple data corruption has occurred. Also, if the wrap around results in other conditions such as buffer overflows, further memory corruption may occur.

**•** Impact: Execute Unauthorized Code or Commands, Bypass Protection Mechanism — Notes: This weakness 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

**•** N/A: Requirements specification: The choice could be made to use a language that is not susceptible to these issues. (Effectiveness: N/A)

**•** Architecture and Design: Provide clear upper and lower bounds on the scale of any protocols designed. (Effectiveness: N/A)

**•** Implementation: Perform validation on all incremented variables to ensure that they remain within reasonable bounds. (Effectiveness: N/A)

## Applicable Platforms

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

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

## Demonstrative Examples

**•** This code intends to allocate a table of size num\_imgs, however as num\_imgs grows large, the calculation determining the size of the list will eventually overflow (CWE-190). This will result in a very small list to be allocated instead. If the subsequent code operates on the list as if it were num\_imgs long, it may result in many types of out-of-bounds problems (CWE-119).

## Notes

**•** Relationship: The relationship between overflow and wrap-around needs to be examined more closely, since several entries (including CWE-190) are closely related.