# CWE Detail – CWE-562

## Description

A function returns the address of a stack variable, which will cause unintended program behavior, typically in the form of a crash.

## Extended Description

Because local variables are allocated on the stack, when a program returns a pointer to a local variable, it is returning a stack address. A subsequent function call is likely to re-use this same stack address, thereby overwriting the value of the pointer, which no longer corresponds to the same variable since a function's stack frame is invalidated when it returns. At best this will cause the value of the pointer to change unexpectedly. In many cases it causes the program to crash the next time the pointer is dereferenced.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Memory, Modify Memory, Execute Unauthorized Code or Commands, DoS: Crash, Exit, or Restart — Notes: If the returned stack buffer address is dereferenced after the return, then an attacker may be able to modify or read memory, depending on how the address is used. If the address is used for reading, then the address itself may be exposed, or the contents that the address points to. If the address is used for writing, this can lead to a crash and possibly code execution.

## Potential Mitigations

**•** Testing: Use static analysis tools to spot return of the address of a stack variable. (Effectiveness: N/A)

## Applicable Platforms

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

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

## Demonstrative Examples

**•** N/A