# CWE Detail – CWE-690

## Description

The product does not check for an error after calling a function that can return with a NULL pointer if the function fails, which leads to a resultant NULL pointer dereference.

## Extended Description

While unchecked return value weaknesses are not limited to returns of NULL pointers (see the examples in CWE-252), functions often return NULL to indicate an error status. When this error condition is not checked, a NULL pointer dereference can occur.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2008-1052: Large Content-Length value leads to NULL pointer dereference when malloc fails.

**•** CVE-2006-6227: Large message length field leads to NULL pointer dereference when malloc fails.

**•** CVE-2006-2555: Parsing routine encounters NULL dereference when input is missing a colon separator.

**•** CVE-2003-1054: URI parsing API sets argument to NULL when a parsing failure occurs, such as when the Referer header is missing a hostname, leading to NULL dereference.

**•** CVE-2008-5183: chain: unchecked return value can lead to NULL dereference

## Modes of Introduction

**•** Implementation: A typical occurrence of this weakness occurs when an application includes user-controlled input to a malloc() call. The related code might be correct with respect to preventing buffer overflows, but if a large value is provided, the malloc() will fail due to insufficient memory. This problem also frequently occurs when a parsing routine expects that certain elements will always be present. If malformed input is provided, the parser might return NULL. For example, strtok() can return NULL.

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart — Notes:

**•** Impact: Execute Unauthorized Code or Commands, Read Memory, Modify Memory — Notes: In rare circumstances, when NULL is equivalent to the 0x0 memory address and privileged code can access it, then writing or reading memory is possible, which may lead to code execution.

## Applicable Platforms

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

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

## Demonstrative Examples

**•** N/A

**•** If an attacker provides an address that appears to be well-formed, but the address does not resolve to a hostname, then the call to gethostbyaddr() will return NULL. Since the code does not check the return value from gethostbyaddr (CWE-252), a NULL pointer dereference (CWE-476) would then occur in the call to strcpy().