# CWE Detail – CWE-240

## Description

The product does not handle or incorrectly handles when two or more structural elements should be consistent, but are not.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2014-0160: Chain: "Heartbleed" bug receives an inconsistent length parameter (CWE-130) enabling an out-of-bounds read (CWE-126), returning memory that could include private cryptographic keys and other sensitive data. (KEV)

**•** CVE-2009-2299: Web application firewall consumes excessive memory when an HTTP request contains a large Content-Length value but no POST data.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context, Unexpected State — Notes:

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** However, the message length variable from the structure is used as the condition for ending the for loop without validating that the message length variable accurately reflects the length of the message body (CWE-606). This can result in a buffer over-read (CWE-125) by reading from memory beyond the bounds of the buffer if the message length variable indicates a length that is longer than the size of a message body (CWE-130).