# CWE Detail – CWE-606

## Description

The product does not properly check inputs that are used for loop conditions, potentially leading to a denial of service or other consequences because of excessive looping.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Resource Consumption (CPU) — Notes:

## Potential Mitigations

**•** Implementation: Do not use user-controlled data for loop conditions. (Effectiveness: N/A)

**•** Implementation: Perform input validation. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A

**•** 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).