# CWE Detail – CWE-707

## Description

The product does not ensure or incorrectly ensures that structured messages or data are well-formed and that certain security properties are met before being read from an upstream component or sent to a downstream component.

## Extended Description

If a message is malformed, it may cause the message to be incorrectly interpreted. Neutralization is an abstract term for any technique that ensures that input (and output) conforms with expectations and is "safe." This can be done by: checking that the input/output is already "safe" (e.g. validation) transformation of the input/output to be "safe" using techniques such as filtering, encoding/decoding, escaping/unescaping, quoting/unquoting, or canonicalization preventing the input/output from being directly provided by an attacker (e.g. "indirect selection" that maps externally-provided values to internally-controlled values) preventing the input/output from being processed at all This weakness typically applies in cases where the product prepares a control message that another process must act on, such as a command or query, and malicious input that was intended as data, can enter the control plane instead. However, this weakness also applies to more general cases where there are not always control implications.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-250
* CAPEC-276
* CAPEC-277
* CAPEC-278
* CAPEC-279
* CAPEC-3
* CAPEC-43
* CAPEC-468
* CAPEC-52
* CAPEC-53
* CAPEC-64
* CAPEC-7
* CAPEC-78
* CAPEC-79
* CAPEC-83
* CAPEC-84

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Other — Notes:

## Applicable Platforms

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

## Notes

**•** Maintenance: Concepts such as validation, data transformation, and neutralization are being refined, so relationships between CWE-20 and other entries such as CWE-707 may change in future versions, along with an update to the Vulnerability Theory document.