# CWE Detail – CWE-924

## Description

The product establishes a communication channel with an endpoint and receives a message from that endpoint, but it does not sufficiently ensure that the message was not modified during transmission.

## Extended Description

Attackers might be able to modify the message and spoof the endpoint by interfering with the data as it crosses the network or by redirecting the connection to a system under their control.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

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

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes: If an attackers can spoof the endpoint, the attacker gains all the privileges that were intended for the original endpoint.

## Applicable Platforms

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

## Notes

**•** Maintenance: This entry should be made more comprehensive in later CWE versions, as it is likely an important design flaw that underlies (or chains to) other weaknesses.