# CWE Detail – CWE-349

## Description

The product, when processing trusted data, accepts any untrusted data that is also included with the trusted data, treating the untrusted data as if it were trusted.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-0018: Does not verify that trusted entity is authoritative for all entities in its response.

**•** CVE-2006-5462: use of extra data in a signature allows certificate signature forging

## Related Attack Patterns (CAPEC)

* CAPEC-141
* CAPEC-142
* CAPEC-75

## Attack TTPs

**•** T1584.002: DNS Server (Tactics: resource-development)

**•** T1557.002: ARP Cache Poisoning (Tactics: credential-access, collection)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Modify Application Data — Notes: An attacker could package untrusted data with trusted data to bypass protection mechanisms to gain access to and possibly modify sensitive data.

## Applicable Platforms

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