# CWE Detail – CWE-923

## Description

The product establishes a communication channel to (or from) an endpoint for privileged or protected operations, but it does not properly ensure that it is communicating with the correct endpoint.

## Extended Description

Attackers might be able to spoof the intended endpoint from a different system or process, thus gaining the same level of access as the intended endpoint. While this issue frequently involves authentication between network-based clients and servers, other types of communication channels and endpoints can have this weakness.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2022-30319: S-bus functionality in a home automation product performs access control using an IP allowlist, which can be bypassed by a forged IP address.

**•** CVE-2022-22547: A troubleshooting tool exposes a web server on a random port between 9000-65535 that could be used for information gathering

**•** CVE-2022-4390: A WAN interface on a router has firewall restrictions enabled for IPv4, but it does not for IPv6, which is enabled by default

**•** CVE-2012-2292: Product has a Silverlight cross-domain policy that does not restrict access to another application, which allows remote attackers to bypass the Same Origin Policy.

**•** CVE-2012-5810: Mobile banking application does not verify hostname, leading to financial loss.

**•** CVE-2014-1266: chain: incorrect "goto" in Apple SSL product bypasses certificate validation, allowing Adversry-in-the-Middle (AITM) attack (Apple "goto fail" bug). CWE-705 (Incorrect Control Flow Scoping) -> CWE-561 (Dead Code) -> CWE-295 (Improper Certificate Validation) -> CWE-393 (Return of Wrong Status Code) -> CWE-300 (Channel Accessible by Non-Endpoint).

**•** CVE-2000-1218: DNS server can accept DNS updates from hosts that it did not query, leading to cache poisoning

## Related Attack Patterns (CAPEC)

* CAPEC-161
* CAPEC-481
* CAPEC-501
* CAPEC-697

## Attack TTPs

**•** T1557.003: DHCP Spoofing (Tactics: credential-access, collection)

**•** T1090.004: Domain Fronting (Tactics: command-and-control)

## 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 attacker 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)

## Demonstrative Examples

**•** Flash crossdomain.xml :

**•** This application does not check the origin of the intent, thus allowing any malicious application to remove a user. Always check the origin of an intent, or create an allowlist of trusted applications using the manifest.xml file.