# CWE Detail – CWE-290

## Description

This attack-focused weakness is caused by incorrectly implemented authentication schemes that are subject to spoofing attacks.

## Extended Description

N/A

## 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-2009-1048: VOIP product allows authentication bypass using 127.0.0.1 in the Host header.

## Related Attack Patterns (CAPEC)

* CAPEC-21
* CAPEC-22
* CAPEC-459
* CAPEC-461
* CAPEC-473
* CAPEC-476
* CAPEC-59
* CAPEC-60
* CAPEC-667
* CAPEC-94

## Attack TTPs

**•** T1557: Adversary-in-the-Middle (Tactics: credential-access, collection)

**•** T1539: Steal Web Session Cookie (Tactics: credential-access)

**•** T1553.002: Code Signing (Tactics: defense-evasion)

**•** T1134.001: Token Impersonation/Theft (Tactics: defense-evasion, privilege-escalation)

**•** T1528: Steal Application Access Token (Tactics: credential-access)

**•** T1036.001: Invalid Code Signature (Tactics: defense-evasion)

**•** T1550.004: Web Session Cookie (Tactics: defense-evasion, lateral-movement)

**•** T1134: Access Token Manipulation (Tactics: defense-evasion, privilege-escalation)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity — Notes: This weakness can allow an attacker to access resources which are not otherwise accessible without proper authentication.

## Demonstrative Examples

**•** The authentication mechanism implemented relies on an IP address for source validation. If an attacker is able to spoof the IP, they may be able to bypass the authentication mechanism.

**•** The code only verifies the address as stored in the request packet. An attacker can spoof this address, thus impersonating a trusted client.

**•** IP addresses are more reliable than DNS names, but they can also be spoofed. Attackers can easily forge the source IP address of the packets they send, but response packets will return to the forged IP address. To see the response packets, the attacker has to sniff the traffic between the victim machine and the forged IP address. In order to accomplish the required sniffing, attackers typically attempt to locate themselves on the same subnet as the victim machine. Attackers may be able to circumvent this requirement by using source routing, but source routing is disabled across much of the Internet today. In summary, IP address verification can be a useful part of an authentication scheme, but it should not be the single factor required for authentication.

## Notes

**•** Relationship: This can be resultant from insufficient verification.