# CWE Detail – CWE-291

## Description

The product uses an IP address for authentication.

## Extended Description

IP addresses can be easily spoofed. Attackers can 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.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## 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.

## Related Attack Patterns (CAPEC)

* CAPEC-4

## Modes of Introduction

**•** Architecture and Design: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

## Common Consequences

**•** Impact: Hide Activities, Gain Privileges or Assume Identity — Notes: Malicious users can fake authentication information, impersonating any IP address.

## Potential Mitigations

**•** Architecture and Design: Use other means of identity verification that cannot be simply spoofed. Possibilities include a username/password or certificate. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

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