# CWE Detail – CWE-941

## Description

The product creates a communication channel to initiate an outgoing request to an actor, but it does not correctly specify the intended destination for that actor.

## Extended Description

Attackers at the destination may be able to spoof trusted servers to steal data or cause a denial of service. There are at least two distinct weaknesses that can cause the product to communicate with an unintended destination: If the product allows an attacker to control which destination is specified, then the attacker can cause it to connect to an untrusted or malicious destination. For example, because UDP is a connectionless protocol, UDP packets can be spoofed by specifying a false source address in the packet; when the server receives the packet and sends a reply, it will specify a destination by using the source of the incoming packet - i.e., the false source. The server can then be tricked into sending traffic to the wrong host, which is effective for hiding the real source of an attack and for conducting a distributed denial of service (DDoS). As another example, server-side request forgery (SSRF) and XML External Entity (XXE) can be used to trick a server into making outgoing requests to hosts that cannot be directly accessed by the attacker due to firewall restrictions. If the product incorrectly specifies the destination, then an attacker who can control this destination might be able to spoof trusted servers. While the most common occurrence is likely due to misconfiguration by an administrator, this can be resultant from other weaknesses. For example, the product might incorrectly parse an e-mail or IP address and send sensitive data to an unintended destination. As another example, an Android application may use a "sticky broadcast" to communicate with a receiver for a particular application, but since sticky broadcasts can be processed by \*any\* receiver, this can allow a malicious application to access restricted data that was only intended for a different application.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Observed Examples (CVEs)

**•** CVE-2013-5211: composite: NTP feature generates large responses (high amplification factor) with spoofed UDP source addresses.

**•** CVE-1999-0513: Classic "Smurf" attack, using spoofed ICMP packets to broadcast addresses.

**•** CVE-1999-1379: DNS query with spoofed source address causes more traffic to be returned to spoofed address than was sent by the attacker.

## Modes of Introduction

**•** Architecture and Design: N/A

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

## Applicable Platforms

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

## Demonstrative Examples

**•** This code sends a DNS record to a requesting IP address. UDP allows the source IP address to be easily changed ('spoofed'), thus allowing an attacker to redirect responses to a target, which may be then be overwhelmed by the network traffic.