# CWE Detail – CWE-406

## Description

The product does not sufficiently monitor or control transmitted network traffic volume, so that an actor can cause the product to transmit more traffic than should be allowed for that actor.

## Extended Description

In the absence of a policy to restrict asymmetric resource consumption, the application or system cannot distinguish between legitimate transmissions and traffic intended to serve as an amplifying attack on target systems. Systems can often be configured to restrict the amount of traffic sent out on behalf of a client, based on the client's origin or access level. This is usually defined in a resource allocation policy. In the absence of a mechanism to keep track of transmissions, the system or application can be easily abused to transmit asymmetrically greater traffic than the request or client should be permitted to.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** 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.

**•** CVE-2000-0041: Large datagrams are sent in response to malformed datagrams.

**•** CVE-1999-1066: Game server sends a large amount.

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

## Modes of Introduction

**•** Operation: N/A

**•** Architecture and Design: If the application uses UDP, then it could potentially be subject to spoofing attacks that use the inherent weaknesses of UDP to perform traffic amplification, although this problem can exist in other protocols or contexts.

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Amplification, DoS: Crash, Exit, or Restart, DoS: Resource Consumption (CPU), DoS: Resource Consumption (Memory), DoS: Resource Consumption (Other) — Notes: System resources can be quickly consumed leading to poor application performance or system crash. This may affect network performance and could be used to attack other systems and applications relying on network performance.

## Potential Mitigations

**•** Architecture and Design: An application must make network resources available to a client commensurate with the client's access level. (Effectiveness: N/A)

**•** Policy: Define a clear policy for network resource allocation and consumption. (Effectiveness: N/A)

**•** Implementation: An application must, at all times, keep track of network resources and meter their usage appropriately. (Effectiveness: N/A)

## 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.

## Notes

**•** Relationship: This can be resultant from weaknesses that simplify spoofing attacks.

**•** Theoretical: Network amplification, when performed with spoofing, is normally a multi-channel attack from attacker (acting as user) to amplifier, and amplifier to victim.