# CWE Detail – CWE-605

## Description

When multiple sockets are allowed to bind to the same port, other services on that port may be stolen or spoofed.

## Extended Description

On most systems, a combination of setting the SO\_REUSEADDR socket option, and a call to bind() allows any process to bind to a port to which a previous process has bound with INADDR\_ANY. This allows a user to bind to the specific address of a server bound to INADDR\_ANY on an unprivileged port, and steal its UDP packets/TCP connection.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: Packets from a variety of network services may be stolen or the services spoofed.

## Potential Mitigations

**•** Policy: Restrict server socket address to known local addresses. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** This code may result in two servers binding a socket to same port, thus receiving each other's traffic. This could be used by an attacker to steal packets meant for another process, such as a secure FTP server.