# CWE Detail – CWE-1327

## Description

The product assigns the address 0.0.0.0 for a database server, a cloud service/instance, or any computing resource that communicates remotely.

## Extended Description

When a server binds to the address 0.0.0.0, it allows connections from every IP address on the local machine, effectively exposing the server to every possible network. This might be much broader access than intended by the developer or administrator, who might only be expecting the server to be reachable from a single interface/network.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2022-21947: Desktop manager for Kubernetes and container management binds a service to 0.0.0.0, allowing users on the network to make requests to a dashboard API.

## Related Attack Patterns (CAPEC)

* CAPEC-1

## Attack TTPs

**•** T1574.010: Services File Permissions Weakness (Tactics: persistence, privilege-escalation, defense-evasion)

## Modes of Introduction

**•** System Configuration: N/A

## Common Consequences

**•** Impact: DoS: Amplification — Notes:

## Potential Mitigations

**•** System Configuration: Assign IP addresses that are not 0.0.0.0. (Effectiveness: High)

**•** System Configuration: Unwanted connections to the configured server may be denied through a firewall or other packet filtering measures. (Effectiveness: High)

## Applicable Platforms

**•** Other (Class: None, Prevalence: Undetermined)

## Demonstrative Examples

**•** The Puppet code snippet is used to provision a signing server that will use 0.0.0.0 to accept traffic. However, as 0.0.0.0 is unrestricted, malicious users may use this IP address to launch frequent requests and cause denial of service attacks.