# CWE Detail – CWE-8

## Description

When an application exposes a remote interface for an entity bean, it might also expose methods that get or set the bean's data. These methods could be leveraged to read sensitive information, or to change data in ways that violate the application's expectations, potentially leading to other vulnerabilities.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data, Modify Application Data — Notes:

## Potential Mitigations

**•** Implementation: Declare Java beans "local" when possible. When a bean must be remotely accessible, make sure that sensitive information is not exposed, and ensure that the application logic performs appropriate validation of any data that might be modified by an attacker. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A

## Notes

**•** Other: Entity beans that expose a remote interface become part of an application's attack surface. For performance reasons, an application should rarely use remote entity beans, so there is a good chance that a remote entity bean declaration is an error.