# CWE Detail – CWE-651

## Description

The Web services architecture may require exposing a Web Service Definition Language (WSDL) file that contains information on the publicly accessible services and how callers of these services should interact with them (e.g. what parameters they expect and what types they return).

## Extended Description

An information exposure may occur if any of the following apply: The WSDL file is accessible to a wider audience than intended. The WSDL file contains information on the methods/services that should not be publicly accessible or information about deprecated methods. This problem is made more likely due to the WSDL often being automatically generated from the code. Information in the WSDL file helps guess names/locations of methods/resources that should not be publicly accessible.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Modes of Introduction

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: The attacker may find sensitive information located in the WSDL file.

## Potential Mitigations

**•** Architecture and Design: Limit access to the WSDL file as much as possible. If services are provided only to a limited number of entities, it may be better to provide WSDL privately to each of these entities than to publish WSDL publicly. (Effectiveness: N/A)

**•** Architecture and Design: Make sure that WSDL does not describe methods that should not be publicly accessible. Make sure to protect service methods that should not be publicly accessible with access controls. (Effectiveness: N/A)

**•** Architecture and Design: Do not use method names in WSDL that might help an adversary guess names of private methods/resources used by the service. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A