# CWE Detail – CWE-1315

## Description

The bus controller enables bits in the fabric end-point to allow responder devices to control transactions on the fabric.

## Extended Description

To support reusability, certain fabric interfaces and end points provide a configurable register bit that allows IP blocks connected to the controller to access other peripherals connected to the fabric. This allows the end point to be used with devices that function as a controller or responder. If this bit is set by default in hardware, or if firmware incorrectly sets it later, a device intended to be a responder on a fabric is now capable of controlling transactions to other devices and might compromise system security.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-1
* CAPEC-180

## Attack TTPs

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

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** System Configuration: N/A

## Common Consequences

**•** Impact: Modify Memory, Read Memory, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: For responder devices, the register bit in the fabric end-point that enables the bus controlling capability must be set to 0 by default. This bit should not be set during secure-boot flows. Also, writes to this register must be access-protected to prevent malicious modifications to obtain bus-controlling capability. (Effectiveness: N/A)

**•** Implementation: For responder devices, the register bit in the fabric end-point that enables the bus controlling capability must be set to 0 by default. This bit should not be set during secure-boot flows. Also, writes to this register must be access-protected to prevent malicious modifications to obtain bus-controlling capability. (Effectiveness: N/A)

**•** System Configuration: For responder devices, the register bit in the fabric end-point that enables the bus controlling capability must be set to 0 by default. This bit should not be set during secure-boot flows. Also, writes to this register must be access-protected to prevent malicious modifications to obtain bus-controlling capability. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The audio-codec chip does not have the bus-controller-enable-register bit hardcoded to 0. There is no platform-firmware flow to verify that the bus-controller-enable bit is set to 0 in all responders.