# CWE Detail – CWE-1276

## Description

Signals between a hardware IP and the parent system design are incorrectly connected causing security risks.

## Extended Description

Individual hardware IP must communicate with the parent system in order for the product to function correctly and as intended. If implemented incorrectly, while not causing any apparent functional issues, may cause security issues. For example, if the IP should only be reset by a system-wide hard reset, but instead the reset input is connected to a software-triggered debug mode reset (which is also asserted during a hard reset), integrity of data inside the IP can be violated.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: This weakness is introduced when integrating IP into a parent design.

## Common Consequences

**•** Impact: Varies by Context — Notes:

## Potential Mitigations

**•** Testing: System-level verification may be used to ensure that components are correctly connected and that design security requirements are not violated due to interactions between various IP blocks. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** In the Verilog code below, the security level input to the TrustZone aware peripheral is correctly driven by an appropriate signal instead of being grounded.

**•** In the above example from HACK@DAC'21, since interrupt signals are not properly connected, the CSR module will fail to send notifications in the event of interrupts. Consequently, critical information in CSR registers that should be flushed or modified in response to an interrupt won't be updated. These vulnerabilities can potentially result in information leakage across various privilege levels.