# CWE Detail – CWE-1189

## Description

The System-On-a-Chip (SoC) does not properly isolate shared resources between trusted and untrusted agents.

## Extended Description

A System-On-a-Chip (SoC) has a lot of functionality, but it may have a limited number of pins or pads. A pin can only perform one function at a time. However, it can be configured to perform multiple different functions. This technique is called pin multiplexing. Similarly, several resources on the chip may be shared to multiplex and support different features or functions. When such resources are shared between trusted and untrusted agents, untrusted agents may be able to access the assets intended to be accessed only by the trusted agents.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2020-8698: Processor has improper isolation of shared resources allowing for information disclosure.

**•** CVE-2019-6260: Baseboard Management Controller (BMC) device implements Advanced High-performance Bus (AHB) bridges that do not require authentication for arbitrary read and write access to the BMC's physical address space from the host, and possibly the network [REF-1138].

## Related Attack Patterns (CAPEC)

* CAPEC-124

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes: If resources being used by a trusted user are shared with an untrusted user, the untrusted user may be able to modify the functionality of the shared resource of the trusted user.

**•** Impact: Quality Degradation — Notes: The functionality of the shared resource may be intentionally degraded.

## Potential Mitigations

**•** Architecture and Design: When sharing resources, avoid mixing agents of varying trust levels. Untrusted agents should not share resources with trusted agents. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** We assume that the threat is from malicious software in
 the untrusted domain. We assume this software has access
 to the core{0-N} memory map and can be running at any
 privilege level on the untrusted cores. The capability
 of this threat in this example is communication to and
 from the mailbox region of SRAM modulated by the
 hrot\_iface. To address this threat, information must not
 enter or exit the shared region of SRAM through
 hrot\_iface when in secure or privileged mode.