# CWE Detail – CWE-1316

## Description

The address map of the on-chip fabric has protected and unprotected regions overlapping, allowing an attacker to bypass access control to the overlapping portion of the protected region.

## Extended Description

Various ranges can be defined in the system-address map, either in the memory or in Memory-Mapped-IO (MMIO) space. These ranges are usually defined using special range registers that contain information, such as base address and size. Address decoding is the process of determining for which range the incoming transaction is destined. To ensure isolation, ranges containing secret data are access-control protected. Occasionally, these ranges could overlap. The overlap could either be intentional (e.g. due to a limited number of range registers or limited choice in choosing size of the range) or unintentional (e.g. introduced by errors). Some hardware designs allow dynamic remapping of address ranges assigned to peripheral MMIO ranges. In such designs, intentional address overlaps can be created through misconfiguration by malicious software. When protected and unprotected ranges overlap, an attacker could send a transaction and potentially compromise the protections in place, violating the principle of least privilege.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2009-4419: Attacker can modify MCHBAR register to overlap with an attacker-controlled region, which modification prevents the SENTER instruction from properly applying VT-d protection while a Measured Launch Environment is being launched.

## Related Attack Patterns (CAPEC)

* CAPEC-456
* CAPEC-679

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Architecture and Design: When architecting the address map of the chip, ensure that protected and unprotected ranges are isolated and do not overlap. When designing, ensure that ranges hardcoded in Register-Transfer Level (RTL) do not overlap. (Effectiveness: N/A)

**•** Implementation: Ranges configured by firmware should not overlap. If overlaps are mandatory because of constraints such as a limited number of registers, then ensure that no assets are present in the overlapped portion. (Effectiveness: N/A)

**•** Testing: Validate mitigation actions with robust testing. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The fabric does not support least privilege, and an attacker can send a transaction to the overlapping region to tamper with user B data.

## Notes

**•** Maintenance: As of CWE 4.6, CWE-1260 and CWE-1316 are siblings under view 1000, but CWE-1260 might be a parent of CWE-1316. More analysis is warranted.