# CWE Detail – CWE-1312

## Description

The firewall in an on-chip fabric protects the main addressed region, but it does not protect any mirrored memory or memory-mapped-IO (MMIO) regions.

## Extended Description

Few fabrics mirror memory and address ranges, where mirrored regions contain copies of the original data. This redundancy is used to achieve fault tolerance. Whatever protections the fabric firewall implements for the original region should also apply to the mirrored regions. If not, an attacker could bypass existing read/write protections by reading from/writing to the mirrored regions to leak or corrupt the original data.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-456
* CAPEC-679

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Architecture and Design: The fabric firewall should apply the same protections as the original region to the mirrored regions. (Effectiveness: N/A)

**•** Implementation: The fabric firewall should apply the same protections as the original region to the mirrored regions. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The firewall only protects the original range but not the mirrored regions.