# CWE Detail – CWE-1252

## Description

The CPU is not configured to provide hardware support for exclusivity of write and execute operations on memory. This allows an attacker to execute data from all of memory.

## Extended Description

CPUs provide a special bit that supports exclusivity of write and execute operations. This bit is used to segregate areas of memory to either mark them as code (instructions, which can be executed) or data (which should not be executed). In this way, if a user can write to a region of memory, the user cannot execute from that region and vice versa. This exclusivity provided by special hardware bit is leveraged by the operating system to protect executable space. While this bit is available in most modern processors by default, in some CPUs the exclusivity is implemented via a memory-protection unit (MPU) and memory-management unit (MMU) in which memory regions can be carved out with exact read, write, and execute permissions. However, if the CPU does not have an MMU/MPU, then there is no write exclusivity. Without configuring exclusivity of operations via segregated areas of memory, an attacker may be able to inject malicious code onto memory and later execute it.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-679

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Architecture and Design: Implement a dedicated bit that can be leveraged by the Operating System to mark data areas as non-executable. If such a bit is not available in the CPU, implement MMU/MPU (memory management unit / memory protection unit). (Effectiveness: N/A)

**•** Integration: If MMU/MPU are not available, then the firewalls need to be implemented in the SoC interconnect to mimic the write-exclusivity operation. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** If the MPU is not configured, then an attacker will be able to inject malicious data into memory and execute it.