# CWE Detail – CWE-1280

## Description

A product's hardware-based access control check occurs after the asset has been accessed.

## Extended Description

The product implements a hardware-based access control check. The asset should be accessible only after the check is successful. If, however, this operation is not atomic and the asset is accessed before the check is complete, the security of the system may be compromised.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-180

## Attack TTPs

**•** T1574.010: Services File Permissions Weakness (Tactics: persistence, privilege-escalation, defense-evasion)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Memory, Read Memory, Modify Application Data, Read Application Data, Gain Privileges or Assume Identity, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Implementation: Implement the access control check first. Access should only be given to asset if agent is authorized. (Effectiveness: N/A)

## Applicable Platforms

**•** Verilog (Class: None, Prevalence: Undetermined)

**•** VHDL (Class: None, Prevalence: Undetermined)

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

## Demonstrative Examples

**•** This code uses Verilog blocking assignments for data\_out and grant\_access. Therefore, these assignments happen sequentially (i.e., data\_out is updated to new value first, and grant\_access is updated the next cycle) and not in parallel. Therefore, the asset data\_out is allowed to be modified even before the access control check is complete and grant\_access signal is set. Since grant\_access does not have a reset value, it will be meta-stable and will randomly go to either 0 or 1.