# CWE Detail – CWE-1037

## Description

The developer builds a security-critical protection mechanism into the software, but the processor optimizes the execution of the program such that the mechanism is removed or modified.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2017-5715: Intel, ARM, and AMD processor optimizations related to speculative execution and branch prediction cause access control checks to be bypassed when placing data into the cache. Often known as "Spectre".

**•** CVE-2017-5753: Intel, ARM, and AMD processor optimizations related to speculative execution and branch prediction cause access control checks to be bypassed when placing data into the cache. Often known as "Spectre".

**•** CVE-2017-5754: Intel processor optimizations related to speculative execution cause access control checks to be bypassed when placing data into the cache. Often known as "Meltdown".

## Related Attack Patterns (CAPEC)

* CAPEC-663

## Modes of Introduction

**•** Architecture and Design: Optimizations built into the design of the processor can have unintended consequences during the execution of an application.

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes: A successful exploitation of this weakness will change the order of an application's execution and will likely be used to bypass specific protection mechanisms. This bypass can be exploited further to potentially read data that should otherwise be unaccessible.

## Applicable Platforms

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

## Notes

**•** Maintenance: As of CWE 4.9, members of the CWE Hardware SIG are closely analyzing this entry and others to improve CWE's coverage of transient execution weaknesses, which include issues related to Spectre, Meltdown, and other attacks. Additional investigation may include other weaknesses related to microarchitectural state. As a result, this entry might change significantly in CWE 4.10.