# CWE Detail – CWE-1038

## Description

The product uses a mechanism that automatically optimizes code, e.g. to improve a characteristic such as performance, but the optimizations can have an unintended side effect that might violate an intended security assumption.

## 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-2008-1685: C compiler optimization, as allowed by specifications, removes code that is used to perform checks to detect integer overflows.

## Modes of Introduction

**•** Architecture and Design: Optimizations built into the design of a product can have unintended consequences during execution.

## Common Consequences

**•** Impact: Alter Execution Logic — Notes: The optimizations alter the order of execution resulting in side effects that were not intended by the original developer.

## Applicable Platforms

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