# CWE Detail – CWE-511

## Description

The product contains code that is designed to disrupt the legitimate operation of the product (or its environment) when a certain time passes, or when a certain logical condition is met.

## Extended Description

When the time bomb or logic bomb is detonated, it may perform a denial of service such as crashing the system, deleting critical data, or degrading system response time. This bomb might be placed within either a replicating or non-replicating Trojan horse.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context, Alter Execution Logic — Notes:

## Potential Mitigations

**•** Installation: Always verify the integrity of the product that is being installed. (Effectiveness: N/A)

**•** Testing: Conduct a code coverage analysis using live testing, then closely inspect any code that is not covered. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A