# CWE Detail – CWE-547

## Description

The product uses hard-coded constants instead of symbolic names for security-critical values, which increases the likelihood of mistakes during code maintenance or security policy change.

## Extended Description

If the developer does not find all occurrences of the hard-coded constants, an incorrect policy decision may be made if one of the constants is not changed. Making changes to these values will require code changes that may be difficult or impossible once the system is released to the field. In addition, these hard-coded values may become available to attackers if the code is ever disclosed.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context, Quality Degradation — Notes: The existence of hardcoded constants could cause unexpected behavior and the introduction of weaknesses during code maintenance or when making changes to the code if all occurrences are not modified. The use of hardcoded constants is an indication of poor quality.

## Potential Mitigations

**•** Implementation: Avoid using hard-coded constants. Configuration files offer a more flexible solution. (Effectiveness: N/A)

## Demonstrative Examples

**•** The following is an example of using a hard-coded constant instead of a symbolic name.