# CWE Detail – CWE-493

## Description

The product has a critical public variable that is not final, which allows the variable to be modified to contain unexpected values.

## Extended Description

If a field is non-final and public, it can be changed once the value is set by any function that has access to the class which contains the field. This could lead to a vulnerability if other parts of the program make assumptions about the contents of that field.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Application Data — Notes: The object could potentially be tampered with.

**•** Impact: Read Application Data — Notes: The object could potentially allow the object to be read.

## Potential Mitigations

**•** Implementation: Declare all public fields as final when possible, especially if it is used to maintain internal state of an Applet or of classes used by an Applet. If a field must be public, then perform all appropriate sanity checks before accessing the field from your code. (Effectiveness: N/A)

## Applicable Platforms

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

**•** C++ (Class: None, Prevalence: Undetermined)

## Demonstrative Examples

**•** The price field is not final. Even though the value is set by the constructor, it could be modified by anybody that has access to an instance of WidgetData.

**•** While this field is readable from any function, and thus might allow an information leak of a pathname, a more serious problem is that it can be changed by any function.