# CWE Detail – CWE-1023

## Description

The product performs a comparison between entities that must consider multiple factors or characteristics of each entity, but the comparison does not include one or more of these factors.

## Extended Description

An incomplete comparison can lead to resultant weaknesses, e.g., by operating on the wrong object or making a security decision without considering a required factor.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2005-2782: PHP remote file inclusion in web application that filters "http" and "https" URLs, but not "ftp".

**•** CVE-2014-6394: Product does not prevent access to restricted directories due to partial string comparison with a public directory

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Alter Execution Logic, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Testing: Thoroughly test the comparison scheme before deploying code into production. Perform positive testing as well as negative testing. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Here, the equals() method only checks the make and model of the Truck objects, but the year of manufacture is not included.

**•** In AuthenticateUser(), the strncmp() call uses the string length of an attacker-provided inPass parameter in order to determine how many characters to check in the password. So, if the attacker only provides a password of length 1, the check will only examine the first byte of the application's password before determining success.