# CWE Detail – CWE-323

## Description

Nonces should be used for the present occasion and only once.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Architecture and Design: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity — Notes: Potentially a replay attack, in which an attacker could send the same data twice, could be crafted if nonces are allowed to be reused. This could allow a user to send a message which masquerades as a valid message from a valid user.

## Potential Mitigations

**•** Implementation: Refuse to reuse nonce values. (Effectiveness: N/A)

**•** Implementation: Use techniques such as requiring incrementing, time based and/or challenge response to assure uniqueness of nonces. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Because the nonce used is always the same, an attacker can impersonate a trusted party by intercepting and resending the encrypted password. This attack avoids the need to learn the unencrypted password.

**•** Once again the nonce used is always the same. An attacker may be able to replay previous legitimate commands or execute new arbitrary commands.