# CWE Detail – CWE-304

## Description

The product implements an authentication technique, but it skips a step that weakens the technique.

## Extended Description

Authentication techniques should follow the algorithms that define them exactly, otherwise authentication can be bypassed or more easily subjected to brute force attacks.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2004-2163: Shared secret not verified in a RADIUS response packet, allowing authentication bypass by spoofing server replies.

**•** CVE-2005-3327: Chain: Authentication bypass by skipping the first startup step as required by the protocol.

## Modes of Introduction

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

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity, Read Application Data, Execute Unauthorized Code or Commands — Notes: This weakness can lead to the exposure of resources or functionality to unintended actors, possibly providing attackers with sensitive information or allowing attackers to execute arbitrary code.

## Applicable Platforms

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