# CWE Detail – CWE-837

## Description

The product requires that an actor should only be able to perform an action once, or to have only one unique action, but the product does not enforce or improperly enforces this restriction.

## Extended Description

In various applications, a user is only expected to perform a certain action once, such as voting, requesting a refund, or making a purchase. When this restriction is not enforced, sometimes this can have security implications. For example, in a voting application, an attacker could attempt to "stuff the ballot box" by voting multiple times. If these votes are counted separately, then the attacker could directly affect who wins the vote. This could have significant business impact depending on the purpose of the product.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2008-0294: Ticket-booking web application allows a user to lock a seat more than once.

**•** CVE-2005-4051: CMS allows people to rate downloads by voting more than once.

**•** CVE-2002-216: Polling software allows people to vote more than once by setting a cookie.

**•** CVE-2003-1433: Chain: lack of validation of a challenge key in a game allows a player to register multiple times and lock other players out of the game.

**•** CVE-2002-1018: Library feature allows attackers to check out the same e-book multiple times, preventing other users from accessing copies of the e-book.

**•** CVE-2009-2346: Protocol implementation allows remote attackers to cause a denial of service (call-number exhaustion) by initiating many message exchanges.

## Common Consequences

**•** Impact: Varies by Context — Notes: An attacker might be able to gain advantage over other users by performing the action multiple times, or affect the correctness of the product.

## Applicable Platforms

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