# CWE Detail – CWE-645

## Description

The product contains an account lockout protection mechanism, but the mechanism is too restrictive and can be triggered too easily, which allows attackers to deny service to legitimate users by causing their accounts to be locked out.

## Extended Description

Account lockout is a security feature often present in applications as a countermeasure to the brute force attack on the password based authentication mechanism of the system. After a certain number of failed login attempts, the users' account may be disabled for a certain period of time or until it is unlocked by an administrator. Other security events may also possibly trigger account lockout. However, an attacker may use this very security feature to deny service to legitimate system users. It is therefore important to ensure that the account lockout security mechanism is not overly restrictive.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Related Attack Patterns (CAPEC)

* CAPEC-2

## Attack TTPs

**•** T1531: Account Access Removal (Tactics: impact)

## Modes of Introduction

**•** Architecture and Design: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

## Common Consequences

**•** Impact: DoS: Resource Consumption (Other) — Notes: Users could be locked out of accounts.

## Potential Mitigations

**•** Architecture and Design: Implement more intelligent password throttling mechanisms such as those which take IP address into account, in addition to the login name. (Effectiveness: N/A)

**•** Architecture and Design: Implement a lockout timeout that grows as the number of incorrect login attempts goes up, eventually resulting in a complete lockout. (Effectiveness: N/A)

**•** Architecture and Design: Consider alternatives to account lockout that would still be effective against password brute force attacks, such as presenting the user machine with a puzzle to solve (makes it do some computation). (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A