# CWE Detail – CWE-832

## Description

The product attempts to unlock a resource that is not locked.

## Extended Description

Depending on the locking functionality, an unlock of a non-locked resource might cause memory corruption or other modification to the resource (or its associated metadata that is used for tracking locks).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2010-4210: function in OS kernel unlocks a mutex that was not previously locked, causing a panic or overwrite of arbitrary memory.

**•** CVE-2008-4302: Chain: OS kernel does not properly handle a failure of a function call (CWE-755), leading to an unlock of a resource that was not locked (CWE-832), with resultant crash.

**•** CVE-2009-1243: OS kernel performs an unlock in some incorrect circumstances, leading to panic.

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart, Execute Unauthorized Code or Commands, Modify Memory, Other — Notes: Depending on the locking being used, an unlock operation might not have any adverse effects. When effects exist, the most common consequence will be a corruption of the state of the product, possibly leading to a crash or exit; depending on the implementation of the unlocking, memory corruption or code execution could occur.