# CWE Detail – CWE-675

## Description

The product performs the same operation on a resource two or more times, when the operation should only be applied once.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2009-0935: Attacker provides invalid address to a memory-reading function, causing a mutex to be unlocked twice

**•** CVE-2019-13351: file descriptor double close can cause the wrong file to be associated with a file descriptor.

**•** CVE-2004-1939: XSS protection mechanism attempts to remove "/" that could be used to close tags, but it can be bypassed using double encoded slashes (%252F)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Other — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** Double free vulnerabilities have two common (and sometimes overlapping) causes:

**•** This code may result in two servers binding a socket to same port, thus receiving each other's traffic. This could be used by an attacker to steal packets meant for another process, such as a secure FTP server.

## Notes

**•** Relationship: This weakness is probably closely associated with other issues related to doubling, such as CWE-462 (duplicate key in alist) or CWE-102 (Struts duplicate validation forms). It's usually a case of an API contract violation (CWE-227).