# CWE Detail – CWE-410

## Description

The product's resource pool is not large enough to handle peak demand, which allows an attacker to prevent others from accessing the resource by using a (relatively) large number of requests for resources.

## Extended Description

Frequently the consequence is a "flood" of connection or sessions.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-1999-1363: Large number of locks on file exhausts the pool and causes crash.

**•** CVE-2001-1340: Product supports only one connection and does not disconnect a user who does not provide credentials.

**•** CVE-2002-0406: Large number of connections without providing credentials allows connection exhaustion.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart, Other — Notes: Floods often cause a crash or other problem besides denial of the resource itself; these are likely examples of \*other\* vulnerabilities, not an insufficient resource pool.

## Potential Mitigations

**•** Architecture and Design: Do not perform resource-intensive transactions for unauthenticated users and/or invalid requests. (Effectiveness: N/A)

**•** Architecture and Design: Consider implementing a velocity check mechanism which would detect abusive behavior. (Effectiveness: N/A)

**•** Operation: Consider load balancing as an option to handle heavy loads. (Effectiveness: N/A)

**•** Implementation: Make sure that resource handles are properly closed when no longer needed. (Effectiveness: N/A)

**•** Architecture and Design: Identify the system's resource intensive operations and consider protecting them from abuse (e.g. malicious automated script which runs the resources out). (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A