# CWE Detail – CWE-799

## Description

The product does not properly limit the number or frequency of interactions that it has with an actor, such as the number of incoming requests.

## Extended Description

This can allow the actor to perform actions more frequently than expected. The actor could be a human or an automated process such as a virus or bot. This could be used to cause a denial of service, compromise program logic (such as limiting humans to a single vote), or other consequences. For example, an authentication routine might not limit the number of times an attacker can guess a password. Or, a web site might conduct a poll but only expect humans to vote a maximum of once a day.

## Threat-Mapped Scoring

Score: 3.1

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2002-1876: Mail server allows attackers to prevent other users from accessing mail by sending large number of rapid requests.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: DoS: Resource Consumption (Other), Bypass Protection Mechanism, Other — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** This code does not place any restriction on the number of authentication attempts made. There should be a limit on the number of authentication attempts made to prevent brute force attacks as in the following example code.