# CWE Detail – CWE-407

## Description

An algorithm in a product has an inefficient worst-case computational complexity that may be detrimental to system performance and can be triggered by an attacker, typically using crafted manipulations that ensure that the worst case is being reached.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2021-32617: C++ library for image metadata has "quadratic complexity" issue with unnecessarily repetitive parsing each time an invalid character is encountered

**•** CVE-2020-10735: Python has "quadratic complexity" issue when converting string to int with many digits in unexpected bases

**•** CVE-2020-5243: server allows ReDOS with crafted User-Agent strings, due to overlapping capture groups that cause excessive backtracking.

**•** CVE-2014-1474: Perl-based email address parser has "quadratic complexity" issue via a string that does not contain a valid address

**•** CVE-2003-0244: CPU consumption via inputs that cause many hash table collisions.

**•** CVE-2003-0364: CPU consumption via inputs that cause many hash table collisions.

**•** CVE-2002-1203: Product performs unnecessary processing before dropping an invalid packet.

**•** CVE-2001-1501: CPU and memory consumption using many wildcards.

**•** CVE-2004-2527: Product allows attackers to cause multiple copies of a program to be loaded more quickly than the program can detect that other copies are running, then exit. This type of error should probably have its own category, where teardown takes more time than initialization.

**•** CVE-2006-6931: Network monitoring system allows remote attackers to cause a denial of service (CPU consumption and detection outage) via crafted network traffic, aka a "backtracking attack."

**•** CVE-2006-3380: Wiki allows remote attackers to cause a denial of service (CPU consumption) by performing a diff between large, crafted pages that trigger the worst case algorithmic complexity.

**•** CVE-2006-3379: Wiki allows remote attackers to cause a denial of service (CPU consumption) by performing a diff between large, crafted pages that trigger the worst case algorithmic complexity.

**•** CVE-2005-2506: OS allows attackers to cause a denial of service (CPU consumption) via crafted Gregorian dates.

**•** CVE-2005-1792: Memory leak by performing actions faster than the software can clear them.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Resource Consumption (CPU), DoS: Resource Consumption (Memory), DoS: Resource Consumption (Other) — Notes: The typical consequence is CPU consumption, but memory consumption and consumption of other resources can also occur.

## Applicable Platforms

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

## Demonstrative Examples

**•** The regular expression has a vulnerable backtracking clause inside (\w+\s?)\*$ which can be triggered to cause a Denial of Service by processing particular phrases. To fix the backtracking problem, backtracking is removed with the ?= portion of the expression which changes it to a lookahead and the \2 which prevents the backtracking. The modified example is: