# CWE Detail – CWE-617

## Description

The product contains an assert() or similar statement that can be triggered by an attacker, which leads to an application exit or other behavior that is more severe than necessary.

## Extended Description

While assertion is good for catching logic errors and reducing the chances of reaching more serious vulnerability conditions, it can still lead to a denial of service. For example, if a server handles multiple simultaneous connections, and an assert() occurs in one single connection that causes all other connections to be dropped, this is a reachable assertion that leads to a denial of service.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2023-49286: Chain: function in web caching proxy does not correctly check a return value (CWE-253) leading to a reachable assertion (CWE-617)

**•** CVE-2006-6767: FTP server allows remote attackers to cause a denial of service (daemon abort) via crafted commands which trigger an assertion failure.

**•** CVE-2006-6811: Chat client allows remote attackers to cause a denial of service (crash) via a long message string when connecting to a server, which causes an assertion failure.

**•** CVE-2006-5779: Product allows remote attackers to cause a denial of service (daemon crash) via LDAP BIND requests with long authcid names, which triggers an assertion failure.

**•** CVE-2006-4095: Product allows remote attackers to cause a denial of service (crash) via certain queries, which cause an assertion failure.

**•** CVE-2006-4574: Chain: security monitoring product has an off-by-one error that leads to unexpected length values, triggering an assertion.

**•** CVE-2004-0270: Anti-virus product has assert error when line length is non-numeric.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart — Notes: An attacker that can trigger an assert statement can still lead to a denial of service if the relevant code can be triggered by an attacker, and if the scope of the assert() extends beyond the attacker's own session.

## Potential Mitigations

**•** Implementation: Make sensitive open/close operation non reachable by directly user-controlled data (e.g. open/close resources) (Effectiveness: N/A)

**•** Implementation: Perform input validation on user data. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A