# CWE Detail – CWE-776

## Description

The product uses XML documents and allows their structure to be defined with a Document Type Definition (DTD), but it does not properly control the number of recursive definitions of entities.

## Extended Description

If the DTD contains a large number of nested or recursive entities, this can lead to explosive growth of data when parsed, causing a denial of service.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2008-3281: XEE in XML-parsing library.

**•** CVE-2011-3288: XML bomb / XEE in enterprise communication product.

**•** CVE-2011-1755: "Billion laughs" attack in XMPP server daemon.

**•** CVE-2009-1955: XML bomb in web server module

**•** CVE-2003-1564: Parsing library allows XML bomb

## Related Attack Patterns (CAPEC)

* CAPEC-197

## Modes of Introduction

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: DoS: Resource Consumption (Other) — Notes: If parsed, recursive entity references allow the attacker to expand data exponentially, quickly consuming all system resources.

## Potential Mitigations

**•** Operation: If possible, prohibit the use of DTDs or use an XML parser that limits the expansion of recursive DTD entities. (Effectiveness: N/A)

**•** Implementation: Before parsing XML files with associated DTDs, scan for recursive entity declarations and do not continue parsing potentially explosive content. (Effectiveness: N/A)

## Applicable Platforms

**•** XML (Class: None, Prevalence: Undetermined)

## Demonstrative Examples

**•** N/A