# CVE Detail – CVE-2008-3281

libxml2 2.6.32 and earlier does not properly detect recursion during entity expansion in an attribute value, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.73108

## CVSS Scoring

CVSS v3.1 Score: 6.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

## CAPEC(s)

* CAPEC-197: Exponential Data Expansion

## Affected Products

* cpe:2.3:a:xmlsoft:libxml2:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apple:safari:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:iphone\_os:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:6.06:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:7.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:7.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:4.7:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:5.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esx:2.5.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esx:2.5.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esx:3.0.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esx:3.0.3:\*:\*:\*:\*:\*:\*:\*