# CVE Detail – CVE-2009-1955

The expat XML parser in the apr\_xml\_\* interface in xml/apr\_xml.c in Apache APR-util before 1.3.7, as used in the mod\_dav and mod\_dav\_svn modules in the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via a crafted XML document containing a large number of nested entity references, as demonstrated by a PROPFIND request, a similar issue to CVE-2003-1564.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.87391

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## 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:apache:apr-util:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:6.06:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:9.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:11:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:http\_server:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apache:http\_server:\*:\*:\*:\*:\*:\*:\*:\*