# CVE Detail – CVE-2012-3489

The xml\_parse function in the libxml2 support in the core server component in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 allows remote authenticated users to determine the existence of arbitrary files or URLs, and possibly obtain file or URL content that triggers a parsing error, via an XML value that refers to (1) a DTD or (2) an entity, related to an XML External Entity (aka XXE) issue.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.7644

## CVSS Scoring

CVSS v3.1 Score: 6.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-611: Improper Restriction of XML External Entity Reference

## CAPEC(s)

* CAPEC-221: Data Serialization External Entities Blowup

## Affected Products

* cpe:2.3:a:postgresql:postgresql:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:postgresql:postgresql:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:postgresql:postgresql:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:postgresql:postgresql:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:12.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:12.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:10.6.8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:10.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:11.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:11.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:12.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:6.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:6.0:\*:\*:\*:\*:\*:\*:\*