# CVE Detail – CVE-2009-2416

Multiple use-after-free vulnerabilities in libxml2 2.5.10, 2.6.16, 2.6.26, 2.6.27, and 2.6.32, and libxml 1.8.17, allow context-dependent attackers to cause a denial of service (application crash) via crafted (1) Notation or (2) Enumeration attribute types in an XML file, as demonstrated by the Codenomicon XML fuzzing framework.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.52554

## CVSS Scoring

CVSS v3.1 Score: 6.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-416: Use After Free

## Affected Products

* cpe:2.3:a:xmlsoft:libxml:1.8.17:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:xmlsoft:libxml2:2.5.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:xmlsoft:libxml2:2.6.16:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:xmlsoft:libxml2:2.6.26:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:xmlsoft:libxml2:2.6.27:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:xmlsoft:libxml2:2.6.32:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:11:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux:5.0:\*:\*:\*:\*:\*:\*:\*
* 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:a:google:chrome:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:apple:safari:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:iphone\_os:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise:10.0:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise:11.0:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vcenter\_server:4.0:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:vmware:vma:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esx:3.0.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esx:3.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esx:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esxi:3.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:vmware:esxi:4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:sun:openoffice.org:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:sun:openoffice.org:\*:\*:\*:\*:\*:\*:\*:\*