# CVE Detail – CVE-2016-3627

The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.4956

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-674: Uncontrolled Recursion

## CAPEC(s)

* CAPEC-230: Serialized Data with Nested Payloads
* CAPEC-231: Oversized Serialized Data Payloads

## Affected Products

* cpe:2.3:o:opensuse:leap:42.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:hp:icewall\_federation\_agent:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:hp:icewall\_file\_manager:3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:xmlsoft:libxml2:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:12.04:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:14.04:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:15.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:16.04:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:a:redhat:jboss\_core\_services:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_desktop:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:7.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:7.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:7.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:7.6:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_eus:7.7:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server\_aus:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server\_aus:7.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server\_aus:7.6:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_workstation:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:vm\_server:3.3:\*:\*:\*:\*:\*:x86:\*
* cpe:2.3:a:oracle:vm\_server:3.4:\*:\*:\*:\*:\*:x86:\*
* cpe:2.3:o:oracle:solaris:11.3:\*:\*:\*:\*:\*:\*:\*