# CVE Detail – CVE-2012-5656

The rasterization process in Inkscape before 0.48.4 allows local users to read arbitrary files via an external entity in a SVG file, aka an XML external entity (XXE) injection attack.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.161

## CVSS Scoring

CVSS v3.1 Score: 5.5

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:inkscape:inkscape:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:16:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:17:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:18:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:10.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:11.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:12.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:12.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:11.4:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:12.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:opensuse:12.2:\*:\*:\*:\*:\*:\*:\*