# CVE Detail – CVE-2012-5821

Lynx does not verify that the server's certificate is signed by a trusted certification authority, which allows man-in-the-middle attackers to spoof SSL servers via a crafted certificate, related to improper use of a certain GnuTLS function.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.46749

## CVSS Scoring

CVSS v3.1 Score: 5.9

Severity: MEDIUM

## Mapped CWE(s)

* CWE-295: Improper Certificate Validation

## CAPEC(s)

* CAPEC-459: Creating a Rogue Certification Authority Certificate
* CAPEC-475: Signature Spoofing by Improper Validation

## Affected Products

* cpe:2.3:a:lynx:lynx:-:\*:\*:\*:\*:\*:\*:\*
* 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:\*:\*:\*:\*:\*:\*:\*