# CVE Detail – CVE-2012-5822

The contribution feature in Zamboni does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate, related to use of the Python urllib2 library.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.35845

## CVSS Scoring

CVSS v3.1 Score: 7.4

Severity: HIGH

## 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:mozilla:zamboni:-:\*:\*:\*:\*:\*:\*:\*