# CVE Detail – CVE-2009-2408

Mozilla Network Security Services (NSS) before 3.12.3, Firefox before 3.0.13, Thunderbird before 2.0.0.23, and SeaMonkey before 1.1.18 do not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority. NOTE: this was originally reported for Firefox before 3.5.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.82021

## 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:mozilla:firefox:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:network\_security\_services:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:seamonkey:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:thunderbird:\*:\*:\*:\*:\*:\*:\*:\*
* 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:o:debian:debian\_linux:5.0:\*:\*:\*:\*:\*:\*:\*
* 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:\*:\*:\*:\*:\*:\*:\*