# CVE Detail – CVE-2008-4989

The \_gnutls\_x509\_verify\_certificate function in lib/x509/verify.c in libgnutls in GnuTLS before 2.6.1 trusts certificate chains in which the last certificate is an arbitrary trusted, self-signed certificate, which allows man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.5943

## 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:gnu:gnutls:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:6.06:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:7.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*
* 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:10:-:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:suse:linux\_enterprise\_server:11:-:\*:\*:\*:\*:\*:\*