# CVE Detail – CVE-2009-0265

Internet Systems Consortium (ISC) BIND 9.6.0 and earlier does not properly check the return value from the OpenSSL EVP\_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077 and CVE-2009-0025.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.5926

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-252: Unchecked Return Value
* 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:isc:bind:\*:\*:\*:\*:\*:\*:\*:\*