# CVE Detail – CVE-2016-2402

OkHttp before 2.7.4 and 3.x before 3.1.2 allows man-in-the-middle attackers to bypass certificate pinning by sending a certificate chain with a certificate from a non-pinned trusted CA and the pinned certificate.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.85216

## 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:squareup:okhttp:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:squareup:okhttp3:3.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:squareup:okhttp3:3.0.0:rc1:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:squareup:okhttp3:3.0.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:squareup:okhttp3:3.1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:squareup:okhttp3:3.1.1:\*:\*:\*:\*:\*:\*:\*