# CVE Detail – CVE-2012-5810

The Chase mobile banking application for Android 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 overriding the default X509TrustManager. NOTE: this vulnerability was fixed in the summer of 2012, but the version number was not changed or is not known.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.30297

## 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:jpmorganchase:chase\_mobile:-:-:\*:\*:\*:android:\*:\*