# CVE Detail – CVE-2006-6679

Pedro Lineu Orso chetcpasswd before 2.4 relies on the X-Forwarded-For HTTP header when verifying a client's status on an IP address ACL, which allows remote attackers to gain unauthorized access by spoofing this header.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.78389

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-863: Incorrect Authorization

## Affected Products

* cpe:2.3:a:chetcpasswd\_project:chetcpasswd:\*:\*:\*:\*:\*:\*:\*:\*