# CWE Detail – CWE-299

## Description

The product does not check or incorrectly checks the revocation status of a certificate, which may cause it to use a certificate that has been compromised.

## Extended Description

An improper check for certificate revocation is a far more serious flaw than related certificate failures. This is because the use of any revoked certificate is almost certainly malicious. The most common reason for certificate revocation is compromise of the system in question, with the result that no legitimate servers will be using a revoked certificate, unless they are sorely out of sync.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2011-2014: LDAP-over-SSL implementation does not check Certificate Revocation List (CRL), allowing spoofing using a revoked certificate.

**•** CVE-2011-0199: Operating system does not check Certificate Revocation List (CRL) in some cases, allowing spoofing using a revoked certificate.

**•** CVE-2010-5185: Antivirus product does not check whether certificates from signed executables have been revoked.

**•** CVE-2009-3046: Web browser does not check if any intermediate certificates are revoked.

**•** CVE-2009-0161: chain: Ruby module for OCSP misinterprets a response, preventing detection of a revoked certificate.

**•** CVE-2011-2701: chain: incorrect parsing of replies from OCSP responders allows bypass using a revoked certificate.

**•** CVE-2011-0935: Router can permanently cache certain public keys, which would allow bypass if the certificate is later revoked.

**•** CVE-2009-1358: chain: OS package manager does not properly check the return value, allowing bypass using a revoked certificate.

**•** CVE-2009-0642: chain: language interpreter does not properly check the return value from an OSCP function, allowing bypass using a revoked certificate.

**•** CVE-2008-4679: chain: web service component does not call the expected method, which prevents a check for revoked certificates.

**•** CVE-2006-4410: Certificate revocation list not searched for certain certificates.

**•** CVE-2006-4409: Product cannot access certificate revocation list when an HTTP proxy is being used.

## Modes of Introduction

**•** Implementation: When the product uses certificate pinning, the developer might not properly validate all relevant components of the certificate before pinning the certificate. This can make it difficult or expensive to test after the pinning is complete.

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes: Trust may be assigned to an entity who is not who it claims to be.

**•** Impact: Other — Notes: Data from an untrusted (and possibly malicious) source may be integrated.

**•** Impact: Read Application Data — Notes: Data may be disclosed to an entity impersonating a trusted entity, resulting in information disclosure.

## Potential Mitigations

**•** Architecture and Design: Ensure that certificates are checked for revoked status. (Effectiveness: N/A)

**•** Implementation: If certificate pinning is being used, ensure that all relevant properties of the certificate are fully validated before the certificate is pinned, including the revoked status. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** Because this code does not use SSL\_get\_verify\_results() to check the certificate, it could accept certificates that have been revoked (X509\_V\_ERR\_CERT\_REVOKED). The product could be communicating with a malicious host.