# CWE Detail – CWE-298

## Description

A certificate expiration is not validated or is incorrectly validated, so trust may be assigned to certificates that have been abandoned due to age.

## Extended Description

When the expiration of a certificate is not taken into account, no trust has necessarily been conveyed through it. Therefore, the validity of the certificate cannot be verified and all benefit of the certificate is lost.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: When the software 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: Other — Notes: The data read from the system vouched for by the expired certificate may be flawed due to malicious spoofing.

**•** Impact: Other — Notes: Trust afforded to the system in question - based on the expired certificate - may allow for spoofing attacks.

## Potential Mitigations

**•** Architecture and Design: Check for expired certificates and provide the user with adequate information about the nature of the problem and how to proceed. (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 expiration. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** If the call to SSL\_get\_verify\_result() returns X509\_V\_ERR\_CERT\_HAS\_EXPIRED, this means that the certificate has expired. As time goes on, there is an increasing chance for attackers to compromise the certificate.