# CWE Detail – CWE-599

## Description

The product uses OpenSSL and trusts or uses a certificate without using the SSL\_get\_verify\_result() function to ensure that the certificate satisfies all necessary security requirements.

## Extended Description

This could allow an attacker to use an invalid certificate to claim to be a trusted host, use expired certificates, or conduct other attacks that could be detected if the certificate is properly validated.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes: The data read may not be properly secured, it might be viewed by an attacker.

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity — Notes: Trust afforded to the system in question may allow for spoofing or redirection attacks.

**•** Impact: Gain Privileges or Assume Identity — Notes: If the certificate is not checked, it may be possible for a redirection or spoofing attack to allow a malicious host with a valid certificate to provide data under the guise of a trusted host. While the attacker in question may have a valid certificate, it may simply be a valid certificate for a different site. In order to ensure data integrity, we must check that the certificate is valid, and that it pertains to the site we wish to access.

## Potential Mitigations

**•** Architecture and Design: Ensure that proper authentication is included in the system design. (Effectiveness: N/A)

**•** Implementation: Understand and properly implement all checks necessary to ensure the identity of entities involved in encrypted communications. (Effectiveness: N/A)

## Demonstrative Examples

**•** Note that the code does not call SSL\_get\_verify\_result(ssl), which effectively disables the validation step that checks the certificate.

## Notes

**•** Relationship: CWE-295 and CWE-599 are very similar, although CWE-599 has a more narrow scope that is only applied to OpenSSL certificates. As a result, other children of CWE-295 can be regarded as children of CWE-599 as well. CWE's use of one-dimensional hierarchical relationships is not well-suited to handle different kinds of abstraction relationships based on concepts like types of resources ("OpenSSL certificate" as a child of "any certificate") and types of behaviors ("not validating expiration" as a child of "improper validation").