# CWE Detail – CWE-593

## Description

The product modifies the SSL context after connection creation has begun.

## Extended Description

If the program modifies the SSL\_CTX object after creating SSL objects from it, there is the possibility that older SSL objects created from the original context could all be affected by that change.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-94

## Attack TTPs

**•** T1557: Adversary-in-the-Middle (Tactics: credential-access, collection)

## Modes of Introduction

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

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes: No authentication takes place in this process, bypassing an assumed protection of encryption.

**•** Impact: Read Application Data — Notes: The encrypted communication between a user and a trusted host may be subject to a sniffing attack.

## Potential Mitigations

**•** Architecture and Design: Use a language or a library that provides a cryptography framework at a higher level of abstraction. (Effectiveness: N/A)

**•** Implementation: Most SSL\_CTX functions have SSL counterparts that act on SSL-type objects. (Effectiveness: N/A)

**•** Implementation: Applications should set up an SSL\_CTX completely, before creating SSL objects from it. (Effectiveness: N/A)

## Demonstrative Examples

**•** N/A