# CWE Detail – CWE-1428

## Description

The product provides or relies on use of HTTP communications when HTTPS is available.

## Extended Description

Because HTTP communications are not encrypted, HTTP is subject to various attacks against confidentiality, integrity, and authenticity. However, unlike many other protocols, HTTPS is widely available as a more secure alternative, because it uses encryption.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Architecture and Design: The product might be designed in a way that assumes that HTTP will be used, e.g., by excluding considerations of encrypted communications between client and server.

**•** Requirements: Product requirements might not include encrypted communications, which could make it easier for designers and developers to choose HTTP.

**•** Implementation: Developers might choose to use unencrypted protocols such as HTTP because they would not require development of additional mechanisms to support encryption, e.g., key or certificate management.

**•** Implementation: When generating content that references web sites such as email messages, ensure that the https:// prefix is included. If a domain name is presented without such a prefix, then clients might automatically treat the link as if it had an "http" prefix. For example, referencing a domain like "mysite.example.com" could cause it to be treated like "http://mysite.example.com", thereby sending unencrypted HTTP requests.

**•** Operation: Designers might assume that the responsibility for encrypted communications might belong to operators and/or network administrators.

## Common Consequences

**•** Impact: Read Application Data, Modify Application Data — Notes: HTTP can be subjected to attacks against confidentiality (by reading cleartext packets); integrity (by modifying sessions); and authenticity (by compromising servers and/or clients using cache poisoning, phishing, or other attacks that enable attackers to spoof a legitimate entity in the communication channel).

## Potential Mitigations

**•** Architecture and Design: Explicitly require HTTPS or another mechanism that ensures that communication is encrypted [REF-1464]. (Effectiveness: N/A)

**•** Implementation: Avoid using "mixed content," i.e., serving a web page over HTTPS in which the page includes elements that use "http:" URLs [REF-1466] [REF-1467]. This is often done for images or other resources that do not seem to have privacy or security implications. (Effectiveness: N/A)

**•** Implementation: Perform "HTTPS forcing," that is, redirecting HTTP requests to HTTPS. (Effectiveness: N/A)

**•** Operation: If the product supports multiple protocols, ensure that encrypted protocols (such as HTTPS) are required, and remove any unencrypted protocols (such as HTTP). (Effectiveness: N/A)

## Applicable Platforms

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