# CWE Detail – CWE-296

## Description

The product does not follow, or incorrectly follows, the chain of trust for a certificate back to a trusted root certificate, resulting in incorrect trust of any resource that is associated with that certificate.

## Extended Description

If a system does not follow the chain of trust of a certificate to a root server, the certificate loses all usefulness as a metric of trust. Essentially, the trust gained from a certificate is derived from a chain of trust -- with a reputable trusted entity at the end of that list. The end user must trust that reputable source, and this reputable source must vouch for the resource in question through the medium of the certificate. In some cases, this trust traverses several entities who vouch for one another. The entity trusted by the end user is at one end of this trust chain, while the certificate-wielding resource is at the other end of the chain. If the user receives a certificate at the end of one of these trust chains and then proceeds to check only that the first link in the chain, no real trust has been derived, since the entire chain must be traversed back to a trusted source to verify the certificate. There are several ways in which the chain of trust might be broken, including but not limited to: Any certificate in the chain is self-signed, unless it the root. Not every intermediate certificate is checked, starting from the original certificate all the way up to the root certificate. An intermediate, CA-signed certificate does not have the expected Basic Constraints or other important extensions. The root certificate has been compromised or authorized to the wrong party.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2016-2402: Server allows bypass of certificate pinning by sending a chain of trust that includes a trusted CA that is not pinned.

**•** CVE-2008-4989: Verification function trusts certificate chains in which the last certificate is self-signed.

**•** CVE-2012-5821: Chain: Web browser uses a TLS-related function incorrectly, preventing it from verifying that a server's certificate is signed by a trusted certification authority (CA).

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

**•** CVE-2009-0265: chain: DNS server does not correctly check return value from the OpenSSL EVP\_VerifyFinal function allows bypass of validation of the certificate chain.

**•** CVE-2009-0124: chain: incorrect check of return value from the OpenSSL EVP\_VerifyFinal function allows bypass of validation of the certificate chain.

**•** CVE-2002-0970: File-transfer software does not validate Basic Constraints of an intermediate CA-signed certificate.

**•** CVE-2002-0862: Cryptographic API, as used in web browsers, mail clients, and other software, does not properly validate Basic Constraints.

## 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: Hide Activities — Notes: Exploitation of this flaw can lead to the trust of data that may have originated with a spoofed source.

**•** Impact: Gain Privileges or Assume Identity, Execute Unauthorized Code or Commands — Notes: Data, requests, or actions taken by the attacking entity can be carried out as a spoofed benign entity.

## Potential Mitigations

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

**•** Implementation: Understand, and properly implement all checks necessary to ensure the integrity of certificate trust integrity. (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 full chain of trust. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** In this case, because the certificate is self-signed, there was no external authority that could prove the identity of the host. The program could be communicating with a different system that is spoofing the host, e.g. by poisoning the DNS cache or using an Adversary-in-the-Middle (AITM) attack to modify the traffic from server to client.