# CWE Detail – CWE-318

## Description

The product stores sensitive information in cleartext in an executable.

## Extended Description

Attackers can reverse engineer binary code to obtain secret data. This is especially easy when the cleartext is plain ASCII. Even if the information is encoded in a way that is not human-readable, certain techniques could determine which encoding is being used, then decode the information.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2005-1794: Product stores RSA private key in a DLL and uses it to sign a certificate, allowing spoofing of servers and Adversary-in-the-Middle (AITM) attacks.

**•** CVE-2001-1527: administration passwords in cleartext in executable

## Related Attack Patterns (CAPEC)

* CAPEC-37
* CAPEC-65

## Attack TTPs

**•** T1040: Network Sniffing (Tactics: credential-access, discovery)

**•** T1005: Data from Local System (Tactics: collection)

**•** T1552.004: Private Keys (Tactics: credential-access)

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes:

## Applicable Platforms

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

## Notes

**•** Terminology: Different people use "cleartext" and "plaintext" to mean the same thing: the lack of encryption. However, within cryptography, these have more precise meanings. Plaintext is the information just before it is fed into a cryptographic algorithm, including already-encrypted text. Cleartext is any information that is unencrypted, although it might be in an encoded form that is not easily human-readable (such as base64 encoding).