# CWE Detail – CWE-313

## Description

The product stores sensitive information in cleartext in a file, or on disk.

## Extended Description

The sensitive information could be read by attackers with access to the file, or with physical or administrator access to the raw disk. 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-2001-1481: Cleartext credentials in world-readable file.

**•** CVE-2005-1828: Password in cleartext in config file.

**•** CVE-2005-2209: Password in cleartext in config file.

**•** CVE-2002-1696: Decrypted copy of a message written to disk given a combination of options and when user replies to an encrypted message.

**•** CVE-2004-2397: Cleartext storage of private key and passphrase in log file when user imports the key.

## Modes of Introduction

**•** Architecture and Design: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

## Common Consequences

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

## Applicable Platforms

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

## Demonstrative Examples

**•** This Java example shows a properties file with a cleartext username / password pair.

## 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).