# CWE Detail – CWE-326

## Description

The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.

## Extended Description

A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2001-1546: Weak encryption

**•** CVE-2004-2172: Weak encryption (chosen plaintext attack)

**•** CVE-2002-1682: Weak encryption

**•** CVE-2002-1697: Weak encryption produces same ciphertext from the same plaintext blocks.

**•** CVE-2002-1739: Weak encryption

**•** CVE-2005-2281: Weak encryption scheme

**•** CVE-2002-1872: Weak encryption (XOR)

**•** CVE-2002-1910: Weak encryption (reversible algorithm).

**•** CVE-2002-1946: Weak encryption (one-to-one mapping).

**•** CVE-2002-1975: Encryption error uses fixed salt, simplifying brute force / dictionary attacks (overlaps randomness).

## Related Attack Patterns (CAPEC)

* CAPEC-112
* CAPEC-192
* CAPEC-20

## Attack TTPs

**•** T1110: Brute Force (Tactics: credential-access)

## Modes of Introduction

**•** Architecture and Design: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Read Application Data — Notes: An attacker may be able to decrypt the data using brute force attacks.

## Potential Mitigations

**•** Architecture and Design: Use an encryption scheme that is currently considered to be strong by experts in the field. (Effectiveness: N/A)

## Applicable Platforms

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