# CWE Detail – CWE-257

## Description

The storage of passwords in a recoverable format makes them subject to password reuse attacks by malicious users. In fact, it should be noted that recoverable encrypted passwords provide no significant benefit over plaintext passwords since they are subject not only to reuse by malicious attackers but also by malicious insiders. If a system administrator can recover a password directly, or use a brute force search on the available information, the administrator can use the password on other accounts.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2022-30018: A messaging platform serializes all elements of User/Group objects, making private information available to adversaries

## Related Attack Patterns (CAPEC)

* CAPEC-49

## Attack TTPs

**•** T1110.001: Password Guessing (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: Gain Privileges or Assume Identity — Notes: User's passwords may be revealed.

**•** Impact: Gain Privileges or Assume Identity — Notes: Revealed passwords may be reused elsewhere to impersonate the users in question.

## Potential Mitigations

**•** Architecture and Design: Use strong, non-reversible encryption to protect stored passwords. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Because a compression algorithm is used instead of a one way hashing algorithm, an attacker can recover compressed passwords stored in the database.

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

## Notes

**•** Maintenance: The meaning of this entry needs to be investigated more closely, especially with respect to what is meant by "recoverable."