# CWE Detail – CWE-261

## Description

Obscuring a password with a trivial encoding does not protect the password.

## Extended Description

Password management issues occur when a password is stored in plaintext in an application's properties or configuration file. A programmer can attempt to remedy the password management problem by obscuring the password with an encoding function, such as base 64 encoding, but this effort does not adequately protect the password.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Related Attack Patterns (CAPEC)

* CAPEC-55

## Attack TTPs

**•** T1110.002: Password Cracking (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:

## Potential Mitigations

**•** N/A: Passwords should be encrypted with keys that are at least 128 bits in length for adequate security. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** This code will run successfully, but anyone with access to config.properties can read the value of password and easily determine that the value has been base 64 encoded. If a devious employee has access to this information, they can use it to break into the system.

**•** This code will run successfully, but anyone who has access to the registry key used to store the password can read the value of password. If a devious employee has access to this information, they can use it to break into the system.

## Notes

**•** Other: The "crypt" family of functions uses weak cryptographic algorithms and should be avoided. It may be present in some projects for compatibility.