# CWE Detail – CWE-256

## Description

Storing a password in plaintext may result in a system compromise.

## Extended Description

Password management issues occur when a password is stored in plaintext in an application's properties, configuration file, or memory. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. In some contexts, even storage of a plaintext password in memory is considered a security risk if the password is not cleared immediately after it is used.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2022-30275: Remote Terminal Unit (RTU) uses a driver that relies on a password stored in plaintext.

## Modes of Introduction

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

**•** Architecture and Design: Developers sometimes believe that they cannot defend the application from someone who has access to the configuration, but this belief makes an attacker's job easier.

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes:

## Potential Mitigations

**•** Architecture and Design: Avoid storing passwords in easily accessible locations. (Effectiveness: N/A)

**•** Architecture and Design: Consider storing cryptographic hashes of passwords as an alternative to storing in plaintext. (Effectiveness: N/A)

**•** N/A: A programmer might 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 because the encoding can be detected and decoded easily. (Effectiveness: None)

## Applicable Platforms

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

## Demonstrative Examples

**•** This code will run successfully, but anyone who has access to config.properties can read the value of password. 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

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

**•** At least one OT product stored a password in plaintext.