# CWE Detail – CWE-260

## Description

The product stores a password in a configuration file that might be accessible to actors who do not know the password.

## Extended Description

This can result in compromise of the system for which the password is used. An attacker could gain access to this file and learn the stored password or worse yet, change the password to one of their choosing.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2022-38665: A continuous delivery pipeline management tool stores an unencypted password in a configuration file.

## Modes of Introduction

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

**•** Implementation: N/A

## 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)

## Applicable Platforms

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

## Demonstrative Examples

**•** Because the LDAP credentials are stored in plaintext, anyone with access to the file can gain access to the resource.

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