# CWE Detail – CWE-262

## Description

The product does not have a mechanism in place for managing password aging.

## Extended Description

Password aging (or password rotation) is a policy that forces users to change their passwords after a defined time period passes, such as every 30 or 90 days. Without mechanisms such as aging, users might not change their passwords in a timely manner. Note that while password aging was once considered an important security feature, it has since fallen out of favor by many, because it is not as effective against modern threats compared to other mechanisms such as slow hashes. In addition, forcing frequent changes can unintentionally encourage users to select less-secure passwords. However, password aging is still in use due to factors such as compliance requirements, e.g., Payment Card Industry Data Security Standard (PCI DSS).

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Related Attack Patterns (CAPEC)

* CAPEC-16
* CAPEC-49
* CAPEC-509
* CAPEC-55
* CAPEC-555
* CAPEC-560
* CAPEC-561
* CAPEC-565
* CAPEC-600
* CAPEC-652
* CAPEC-653
* CAPEC-70

## Attack TTPs

**•** T1110.001: Password Guessing (Tactics: credential-access)

**•** T1133: External Remote Services (Tactics: persistence, initial-access)

**•** T1110.002: Password Cracking (Tactics: credential-access)

**•** T1558: Steal or Forge Kerberos Tickets (Tactics: credential-access)

**•** T1021.002: SMB/Windows Admin Shares (Tactics: lateral-movement)

**•** T1021: Remote Services (Tactics: lateral-movement)

**•** T1078.001: Default Accounts (Tactics: defense-evasion, persistence, privilege-escalation, initial-access)

**•** T1110.003: Password Spraying (Tactics: credential-access)

**•** T1078: Valid Accounts (Tactics: defense-evasion, persistence, privilege-escalation, initial-access)

**•** T1110.004: Credential Stuffing (Tactics: credential-access)

**•** T1114.002: Remote Email Collection (Tactics: collection)

**•** T1558.003: Kerberoasting (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: As passwords age, the probability that they are compromised grows.

## Potential Mitigations

**•** Architecture and Design: As part of a product's design, require users to change their passwords regularly and avoid reusing previous passwords. (Effectiveness: N/A)

**•** Implementation: Developers might disable clipboard paste operations into password fields as a way to discourage users from pasting a password into a clipboard. However, this might encourage users to choose less-secure passwords that are easier to type, and it can reduce the usability of password managers [REF-1294]. (Effectiveness: Discouraged Common Practice)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A