# CWE Detail – CWE-309

## Description

The use of password systems as the primary means of authentication may be subject to several flaws or shortcomings, each reducing the effectiveness of the mechanism.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 3.0

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: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity — Notes: A password authentication mechanism error will almost always result in attackers being authorized as valid users.

## Potential Mitigations

**•** Architecture and Design: In order to protect password systems from compromise, the following should be noted: Passwords should be stored safely to prevent insider attack and to ensure that -- if a system is compromised -- the passwords are not retrievable. Due to password reuse, this information may be useful in the compromise of other systems these users work with. In order to protect these passwords, they should be stored encrypted, in a non-reversible state, such that the original text password cannot be extracted from the stored value. Password aging should be strictly enforced to ensure that passwords do not remain unchanged for long periods of time. The longer a password remains in use, the higher the probability that it has been compromised. For this reason, passwords should require refreshing periodically, and users should be informed of the risk of passwords which remain in use for too long. Password strength should be enforced intelligently. Rather than restrict passwords to specific content, or specific length, users should be encouraged to use upper and lower case letters, numbers, and symbols in their passwords. The system should also ensure that no passwords are derived from dictionary words. (Effectiveness: N/A)

**•** Architecture and Design: Use a zero-knowledge password protocol, such as SRP. (Effectiveness: N/A)

**•** Architecture and Design: Ensure that passwords are stored safely and are not reversible. (Effectiveness: N/A)

**•** Architecture and Design: Implement password aging functionality that requires passwords be changed after a certain point. (Effectiveness: N/A)

**•** Architecture and Design: Use a mechanism for determining the strength of a password and notify the user of weak password use. (Effectiveness: N/A)

**•** Architecture and Design: Inform the user of why password protections are in place, how they work to protect data integrity, and why it is important to heed their warnings. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** This code relies exclusively on a password mechanism (CWE-309) using only one factor of authentication (CWE-308). If an attacker can steal or guess a user's password, they are given full access to their account. Note this code also uses SHA-1, which is a weak hash (CWE-328). It also does not use a salt (CWE-759).