# CWE Detail – CWE-308

## Description

The use of single-factor authentication can lead to unnecessary risk of compromise when compared with the benefits of a dual-factor authentication scheme.

## Extended Description

While the use of multiple authentication schemes is simply piling on more complexity on top of authentication, it is inestimably valuable to have such measures of redundancy. The use of weak, reused, and common passwords is rampant on the internet. Without the added protection of multiple authentication schemes, a single mistake can result in the compromise of an account. For this reason, if multiple schemes are possible and also easy to use, they should be implemented and required.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2022-35248: Chat application skips validation when Central Authentication Service
 (CAS) is enabled, effectively removing the second factor from
 two-factor authentication

## Related Attack Patterns (CAPEC)

* CAPEC-16
* CAPEC-49
* CAPEC-509
* CAPEC-55
* CAPEC-555
* CAPEC-560
* CAPEC-561
* CAPEC-565
* CAPEC-600
* CAPEC-644
* CAPEC-645
* 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)

**•** T1550.003: Pass the Ticket (Tactics: defense-evasion, lateral-movement)

**•** 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)

**•** T1550.002: Pass the Hash (Tactics: defense-evasion, lateral-movement)

**•** 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: Bypass Protection Mechanism — Notes: If the secret in a single-factor authentication scheme gets compromised, full authentication is possible.

## Potential Mitigations

**•** Architecture and Design: Use multiple independent authentication schemes, which ensures that -- if one of the methods is compromised -- the system itself is still likely safe from compromise. (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).