# CWE Detail – CWE-1390

## Description

The product uses an authentication mechanism to restrict access to specific users or identities, but the mechanism does not sufficiently prove that the claimed identity is correct.

## Extended Description

Attackers may be able to bypass weak authentication faster and/or with less effort than expected.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2022-30034: Chain: Web UI for a Python RPC framework does not use regex anchors to validate user login emails (CWE-777), potentially allowing bypass of OAuth (CWE-1390).

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

**•** CVE-2021-3116: Chain: Python-based HTTP Proxy server uses the wrong boolean operators (CWE-480) causing an incorrect comparison (CWE-697) that identifies an authN failure if all three conditions are met instead of only one, allowing bypass of the proxy authentication (CWE-1390)

**•** CVE-2022-29965: Distributed Control System (DCS) uses a deterministic algorithm to generate utility passwords

**•** CVE-2022-29959: Initialization file contains credentials that can be decoded using a "simple string transformation"

**•** CVE-2020-8994: UART interface for AI speaker uses empty password for root shell

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data, Gain Privileges or Assume Identity, Execute Unauthorized Code or Commands — Notes: This weakness can lead to the exposure of resources or functionality to unintended actors, possibly providing attackers with sensitive information or even execute arbitrary code.

## Applicable Platforms

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

## Demonstrative Examples

**•** Multiple OT products used weak authentication.