# CWE Detail – CWE-1391

## Description

The product uses weak credentials (such as a default key or hard-coded password) that can be calculated, derived, reused, or guessed by an attacker.

## Extended Description

By design, authentication protocols try to ensure that attackers must perform brute force attacks if they do not know the credentials such as a key or password. However, when these credentials are easily predictable or even fixed (as with default or hard-coded passwords and keys), then the attacker can defeat the mechanism without relying on brute force. Credentials may be weak for different reasons, such as: Hard-coded (i.e., static and unchangeable by the administrator) Default (i.e., the same static value across different deployments/installations, but able to be changed by the administrator) Predictable (i.e., generated in a way that produces unique credentials across deployments/installations, but can still be guessed with reasonable efficiency) Even if a new, unique credential is intended to be generated for each product installation, if the generation is predictable, then that may also simplify guessing attacks.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** [REF-1374]: Chain: JavaScript-based cryptocurrency library can fall back to the insecure Math.random() function instead of reporting a failure (CWE-392), thus reducing the entropy (CWE-332) and leading to generation of non-unique cryptographic keys for Bitcoin wallets (CWE-1391)

**•** CVE-2022-30270: Remote Terminal Unit (RTU) uses default credentials for some SSH accounts

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

**•** CVE-2022-30271: Remote Terminal Unit (RTU) uses a hard-coded SSH private key that is likely to be used in typical deployments

**•** CVE-2021-38759: microcontroller board has default password, allowing admin access

**•** CVE-2021-41192: data visualization/sharing package uses default secret keys or cookie values if they are not specified in environment variables

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

**•** CVE-2020-27020: password manager does not generate cryptographically strong passwords, allowing prediction of passwords using guessable details such as time of generation

**•** CVE-2020-8632: password generator for cloud application has small length value, making it easier for brute-force guessing

**•** CVE-2020-5365: network-attached storage (NAS) system has predictable default passwords for a diagnostics/support account

**•** CVE-2020-5248: IT asset management app has a default encryption key that is the same across installations

**•** CVE-2018-3825: cloud cluster management product has a default master encryption key

**•** CVE-2012-3503: Installation script has a hard-coded secret token value, allowing attackers to bypass authentication

**•** CVE-2010-2306: Intrusion Detection System (IDS) uses the same static, private SSL keys for multiple devices and installations, allowing decryption of SSL traffic

**•** CVE-2001-0618: Residential gateway uses the last 5 digits of the 'Network Name' or SSID as the default WEP key, which allows attackers to get the key by sniffing the SSID, which is sent in the clear

## Modes of Introduction

**•** Requirements: N/A

**•** Architecture and Design: N/A

**•** Installation: N/A

**•** Operation: N/A

## Applicable Platforms

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

## Demonstrative Examples

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