# CWE Detail – CWE-1393

## Description

The product uses default passwords for potentially critical functionality.

## Extended Description

It is common practice for products to be designed to use  
 default passwords for authentication. The rationale is to  
 simplify the manufacturing process or the system  
 administrator's task of installation and deployment into an  
 enterprise. However, if admins do not change the defaults,  
 then it makes it easier for attackers to quickly bypass  
 authentication across multiple organizations. There are many  
 lists of default passwords and default-password scanning tools  
 that are easily available from the World Wide Web.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

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

**•** CVE-2022-2336: OPC Unified Architecture (OPC UA) industrial automation product has a default password

**•** CVE-2021-38759: microcontroller board has default password

**•** CVE-2021-44480: children's smart watch has default passwords allowing attackers to send SMS commands and listen to the device's surroundings

**•** CVE-2020-11624: surveillance camera has default password for the admin account

**•** CVE-2018-15719: medical dental records product installs a MySQL database with a blank default password

**•** CVE-2014-9736: healthcare system for archiving patient images has default passwords for key management and storage databases

**•** CVE-2000-1209: database product installs admin account with default null password, allowing privileges, as exploited by various worms

## Modes of Introduction

**•** Architecture and Design: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity — Notes:

## Potential Mitigations

**•** Requirements: Prohibit use of default, hard-coded, or other values that do not vary for each installation of the product - especially for separate organizations. (Effectiveness: High)

**•** Documentation: Ensure that product documentation clearly emphasizes the presence of default passwords and provides steps for the administrator to change them. (Effectiveness: Limited)

**•** Architecture and Design: Force the administrator to change the credential upon installation. (Effectiveness: High)

**•** Installation: The product administrator could change the defaults upon installation or during operation. (Effectiveness: Moderate)

## Applicable Platforms

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

## Demonstrative Examples

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