# CWE Detail – CWE-1394

## Description

The product uses a default cryptographic key for potentially critical functionality.

## Extended Description

It is common practice for products to be designed to use
 default keys. 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, it is easier for attackers to bypass
 authentication quickly across multiple organizations.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

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

**•** CVE-2016-1561: backup storage product has a default SSH public key in the authorized\_keys file, allowing root access

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

## 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)

**•** 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)