# CWE Detail – CWE-321

## Description

The product uses a hard-coded, unchangeable cryptographic key.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2022-29960: Engineering Workstation uses hard-coded cryptographic keys that could allow for unathorized filesystem access and privilege escalation

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

**•** CVE-2020-10884: WiFi router service has a hard-coded encryption key, allowing root access

**•** CVE-2014-2198: Communications / collaboration product has a hardcoded SSH private key, allowing access to root account

## Modes of Introduction

**•** Architecture and Design: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity, Read Application Data — Notes: If hard-coded cryptographic keys are used, it is almost certain that malicious users will gain access through the account in question. The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered.

## Potential Mitigations

**•** Architecture and Design: Prevention schemes mirror that of hard-coded password storage. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The cryptographic key is within a hard-coded string value that is compared to the password. It is likely that an attacker will be able to read the key and compromise the system.

**•** Multiple vendors used hard-coded keys for critical functionality in their OT products.

## Notes

**•** Other: The main difference between the use of hard-coded passwords and the use of hard-coded cryptographic keys is the false sense of security that the former conveys. Many people believe that simply hashing a hard-coded password before storage will protect the information from malicious users. However, many hashes are reversible (or at least vulnerable to brute force attacks) -- and further, many authentication protocols simply request the hash itself, making it no better than a password.

**•** Maintenance: The Taxonomy\_Mappings to ISA/IEC 62443 were added in CWE 4.10, but they are still under review and might change in future CWE versions. These draft mappings were performed by members of the "Mapping CWE to 62443" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG), and their work is incomplete as of CWE 4.10. The mappings are included to facilitate discussion and review by the broader ICS/OT community, and they are likely to change in future CWE versions.