# CWE Detail – CWE-1242

## Description

The device includes chicken bits or undocumented features that can create entry points for unauthorized actors.

## Extended Description

A common design practice is to use undocumented bits on a device that can be used to disable certain functional security features. These bits are commonly referred to as "chicken bits". They can facilitate quick identification and isolation of faulty components, features that negatively affect performance, or features that do not provide the required controllability for debug and test. Another way to achieve this is through implementation of undocumented features. An attacker might exploit these interfaces for unauthorized access.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-212
* CAPEC-36

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Documentation: N/A

## Common Consequences

**•** Impact: Modify Memory, Read Memory, Execute Unauthorized Code or Commands, Gain Privileges or Assume Identity, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: The implementation of chicken bits in a released product is highly discouraged. If implemented at all, ensure that they are disabled in production devices. All interfaces to a device should be documented. (Effectiveness: High)

## Applicable Platforms

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

## Demonstrative Examples

**•** Remove all chicken bits and hidden features that are exposed to attackers. Add authorization schemes that rely on cryptographic primitives to access any features that the manufacturer does not want to expose. Clearly document all interfaces.