# CWE Detail – CWE-1243

## Description

Access to security-sensitive information stored in fuses is not limited during debug.

## Extended Description

Several security-sensitive values are programmed into fuses to be used during early-boot flows or later at runtime. Examples of these security-sensitive values include root keys, encryption keys, manufacturing-specific information, chip-manufacturer-specific information, and original-equipment-manufacturer (OEM) data. After the chip is powered on, these values are sensed from fuses and stored in temporary locations such as registers and local memories. These locations are typically access-control protected from untrusted agents capable of accessing them. Even to trusted agents, only read-access is provided. However, these locations are not blocked during debug operations, allowing a user to access this sensitive information.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Related Attack Patterns (CAPEC)

* CAPEC-116
* CAPEC-545

## Attack TTPs

**•** T1555.001: Keychain (Tactics: credential-access)

**•** T1005: Data from Local System (Tactics: collection)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Memory, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Disable access to security-sensitive information stored in fuses directly and also reflected from temporary storage locations when in debug mode. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

**•** The above code illustrates an instance of a vulnerable implementation for blocking AES key mechanism when the system is in debug mode (i.e., when debug\_mode\_i is asserted). During debug mode, key accesses through key\_big0 and key\_big1 are effectively disconnected, as their values are set to zero. However, the key accessed via the key\_big2 signal remains accessible, creating a potential pathway for sensitive fuse data leakage, specifically AES key2, during debug mode. Furthermore, even though it is not strictly necessary to disconnect the key\_big signal when entering debug mode (since disconnecting key\_big0, key\_big1, and key\_big2 will inherently disconnect key\_big), it is advisable, in line with the defense-in-depth strategy, to also sever the connection to key\_big. This additional security measure adds an extra layer of protection and safeguards the AES keys against potential future modifications to the key\_big logic.