# CWE Detail – CWE-1231

## Description

The product uses a trusted lock bit for restricting access to registers, address regions, or other resources, but the product does not prevent the value of the lock bit from being modified after it has been set.

## Extended Description

In integrated circuits and hardware
 intellectual property (IP) cores, device configuration
 controls are commonly programmed after a device power
 reset by a trusted firmware or software module (e.g.,
 BIOS/bootloader) and then locked from any further
 modification. This behavior is commonly implemented using a trusted lock bit.
 When set, the lock bit disables writes to a protected set of
 registers or address regions. Design or coding errors in
 the implementation of the lock bit protection feature
 may allow the lock bit to be modified or cleared by
 software after it has been set. Attackers might be able to unlock the system and
 features that the bit is intended to protect.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2017-6283: chip reset clears critical read/write lock permissions for RSA function

## Related Attack Patterns (CAPEC)

* CAPEC-680

## Modes of Introduction

**•** Architecture and Design: Such issues could be introduced during hardware architecture and design and identified later during Testing or System Configuration phases.

**•** Implementation: Such issues could be introduced during implementation and identified later during Testing or System Configuration phases.

## Common Consequences

**•** Impact: Modify Memory — Notes: Registers protected by lock bit can be modified even when lock is set.

## Potential Mitigations

**•** Architecture and Design: Security lock bit protections must be reviewed for design inconsistency and common weaknesses. Security lock programming flow and lock properties must be tested in pre-silicon and post-silicon testing. (Effectiveness: High)

## Applicable Platforms

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

## Demonstrative Examples

**•** In this example, note that if the system heats to critical temperature, the response of the system is controlled by the TEMP\_HW\_SHUTDOWN bit [1], which is not lockable. Thus, the intended security property of the critical temperature sensor cannot be fully protected, since software can misconfigure the TEMP\_HW\_SHUTDOWN register even after the lock bit is set to disable the shutdown response.

**•** In the vulnerable code, the reglk\_mem is used for locking information. If one of its bits toggle to 1, the corresponding peripheral's registers will be locked. In the context of the HACK@DAC System-on-Chip (SoC), it is pertinent to note the existence of two distinct categories of reset signals.