# CWE Detail – CWE-1233

## Description

The product uses a register lock bit protection mechanism, but it does not ensure that the lock bit prevents modification of system registers or controls that perform changes to important hardware system configuration.

## Extended Description

Integrated circuits and hardware intellectual properties (IPs) might provide device configuration controls that need to be programmed after device power reset by a trusted firmware or software module, commonly set by BIOS/bootloader. After reset, there can be an expectation that the controls cannot be used to perform any further modification. This behavior is commonly implemented using a trusted lock bit, which can be set to disable writes to a protected set of registers or address regions. The lock protection is intended to prevent modification of certain system configuration (e.g., memory/memory protection unit configuration). However, if the lock bit does not effectively write-protect all system registers or controls that could modify the protected system configuration, then an adversary may be able to use software to access the registers/controls and modify the protected hardware configuration.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2018-9085: Certain servers leave a write protection lock bit  
 unset after boot, potentially allowing modification of  
 parts of flash memory.

**•** CVE-2014-8273: Chain: chipset has a race condition (CWE-362) between when an interrupt handler detects an attempt to write-enable the BIOS (in violation of the lock bit), and when the handler resets the write-enable bit back to 0, allowing attackers to issue BIOS writes during the timing window [REF-1237].

## Related Attack Patterns (CAPEC)

* CAPEC-176
* 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: System Configuration protected by the lock bit can be modified even when the 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: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** In this example note that only the CRITICAL\_TEMP\_LIMIT register is protected by the TEMP\_SENSOR\_LOCK bit, while the security design intent is to protect any modification of the critical temperature detection and response. The response of the system, if the system heats to a critical temperature, is controlled by TEMP\_HW\_SHUTDOWN bit [1], which is not lockable. Also, the TEMP\_SENSOR\_CALIB register is not protected by the lock bit. By modifying the temperature sensor calibration, the conversion of the sensor data to a degree centigrade can be changed, such that the current temperature will never be detected to exceed critical temperature value programmed by the protected lock. Similarly, by modifying the TEMP\_HW\_SHUTDOWN.Enable bit, the system response detection of the current temperature exceeding critical temperature can be disabled.