# CWE Detail – CWE-1234

## Description

System configuration protection may be bypassed during debug mode.

## Extended Description

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 is commonly implemented using a trusted lock bit, which when set, disables 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). If debug features supported by hardware or internal modes/system states are supported in the hardware design, modification of the lock protection may be allowed allowing access and modification of configuration information.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-176

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes: Bypass of lock bit allows access and modification of system configuration even when the lock bit is set.

## Potential Mitigations

**•** Architecture and Design: Security Lock bit protections should be reviewed for any bypass/override modes supported. Any supported override modes either should be removed or protected using authenticated debug modes. Security lock programming flow and lock properties should be tested in pre-silicon and post-silicon testing. (Effectiveness: High)

## Applicable Platforms

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

## Demonstrative Examples

**•** If either the scan\_mode or the debug\_unlocked modes can be triggered by software, then the lock protection may be bypassed.

**•** The example code [REF-1375] illustrates an instance of a vulnerable implementation of register locks in the SoC. In this flawed implementation [REF-1375], the reglk\_mem registers are also being reset when the system enters debug mode (indicated by the jtag\_unlock signal). Consequently, users can simply put the processor in debug mode to access sensitive contents that are supposed to be protected by the register lock feature.