# CWE Detail – CWE-1274

## Description

The product conducts a secure-boot process that transfers bootloader code from Non-Volatile Memory (NVM) into Volatile Memory (VM), but it does not have sufficient access control or other protections for the Volatile Memory.

## Extended Description

Adversaries could bypass the secure-boot process and execute their own untrusted, malicious boot code. As a part of a secure-boot process, the read-only-memory (ROM) code for a System-on-Chip (SoC) or other system fetches bootloader code from Non-Volatile Memory (NVM) and stores the code in Volatile Memory (VM), such as dynamic, random-access memory (DRAM) or static, random-access memory (SRAM). The NVM is usually external to the SoC, while the VM is internal to the SoC. As the code is transferred from NVM to VM, it is authenticated by the SoC's ROM code. If the volatile-memory-region protections or access controls are insufficient to prevent modifications from an adversary or untrusted agent, the secure boot may be bypassed or replaced with the execution of an adversary's code.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2019-2267: Locked memory regions may be modified through other interfaces in a secure-boot-loader image due to improper access control.

## Related Attack Patterns (CAPEC)

* CAPEC-456
* CAPEC-679

## Modes of Introduction

**•** Architecture and Design: This weakness can be introduced during hardware architecture or design but can be identified later during testing.

## Common Consequences

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

## Potential Mitigations

**•** Architecture and Design: Ensure that the design of volatile-memory protections is enough to prevent modification from an adversary or untrusted code. (Effectiveness: N/A)

**•** Testing: Test the volatile-memory protections to ensure they are safe from modification or untrusted code. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The memory from where the boot loader executes can be modified by an adversary.