# CWE Detail – CWE-1328

## Description

Security-version number in hardware is mutable, resulting in the ability to downgrade (roll-back) the boot firmware to vulnerable code versions.

## Extended Description

A System-on-Chip (SoC) implements secure boot or verified boot. It might support a security version number, which prevents downgrading the current firmware to a vulnerable version. Once downgraded to a previous version, an adversary can launch exploits on the SoC and thus compromise the security of the SoC. These downgrade attacks are also referred to as roll-back attacks. The security version number must be stored securely and persistently across power-on resets. A common weakness is that the security version number is modifiable by an adversary, allowing roll-back or downgrade attacks or, under certain circumstances, preventing upgrades (i.e. Denial-of-Service on upgrades). In both cases, the SoC is in a vulnerable state.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-176

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: Such issues could be introduced during hardware architecture and design, and can be identified later during testing or system configuration phases.

## Common Consequences

**•** Impact: Other — Notes: Impact includes roll-back or downgrade to a vulnerable version of the firmware or DoS (prevent upgrades).

## Potential Mitigations

**•** Architecture and Design: When architecting the system, security version data should be designated for storage in registers that are either read-only or have access controls that prevent modification by an untrusted agent. (Effectiveness: N/A)

**•** Implementation: During implementation and test, security version data should be demonstrated to be read-only and access controls should be validated. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** In general, if the security version number is mutable, the implementation is vulnerable. A mutable security version number allows an adversary to change the security version to a lower value to allow roll-back or to a higher value to prevent future upgrades.