# CWE Detail – CWE-1283

## Description

The register contents used for attestation or measurement reporting data to verify boot flow are modifiable by an adversary.

## Extended Description

A System-on-Chip (SoC) implements secure boot or verified boot. During this boot flow, the SoC often measures the code that it authenticates. The measurement is usually done by calculating the one-way hash of the code binary and extending it to the previous hash. The hashing algorithm should be a Secure One-Way hash function. The final hash, i.e., the value obtained after the completion of the boot flow, serves as the measurement data used in reporting or in attestation. The calculated hash is often stored in registers that can later be read by the party of interest to determine tampering of the boot flow. A common weakness is that the contents in these registers are modifiable by an adversary, thus spoofing the measurement.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-680

## Modes of Introduction

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

**•** Implementation: If the access-controls which protecting the reporting registers are misconfigured during implementation, this weakness can arise.

## Common Consequences

**•** Impact: Read Memory, Read Application Data — Notes:

## Potential Mitigations

**•** Architecture and Design: Measurement data should be stored in registers that are read-only or otherwise have access controls that prevent modification by an untrusted agent. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** To prevent the above scenario, the registers should have one or more of the following properties: Should be Read-Only with respect to an adversary Cannot be extended or modifiable either directly or indirectly (using a trusted agent as proxy) by an adversary Should have appropriate access controls or protections

## Notes

**•** Maintenance: This entry is still in development and will continue to see updates and content improvements.