# CWE Detail – CWE-1282

## Description

Immutable data, such as a first-stage bootloader, device identifiers, and "write-once" configuration settings are stored in writable memory that can be re-programmed or updated in the field.

## Extended Description

Security services such as secure boot, authentication of code and data, and device attestation all require assets such as the first stage bootloader, public keys, golden hash digests, etc. which are implicitly trusted. Storing these assets in read-only memory (ROM), fuses, or one-time programmable (OTP) memory provides strong integrity guarantees and provides a root of trust for securing the rest of the system. Security is lost if assets assumed to be immutable can be modified.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-458
* CAPEC-679

## Modes of Introduction

**•** Implementation: Keys, code, configuration settings, and other data should be programmed in write-once or read-only memory instead of writable memory.

## Common Consequences

**•** Impact: Varies by Context — Notes:

## Potential Mitigations

**•** Implementation: All immutable code or data should be programmed into ROM or write-once memory. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

## Notes

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

**•** Maintenance: As of CWE 4.3, CWE-1282 and CWE-1233 are being investigated
 for potential duplication or overlap.