# CWE Detail – CWE-1246

## Description

The product does not implement or incorrectly implements wear leveling operations in limited-write non-volatile memories.

## Extended Description

Non-volatile memories such as NAND Flash, EEPROM, etc. have individually erasable segments, each of which can be put through a limited number of program/erase or write cycles. For example, the device can only endure a limited number of writes, after which the device becomes unreliable. In order to wear out the cells in a uniform manner, non-volatile memory and storage products based on the above-mentioned technologies implement a technique called wear leveling. Once a set threshold is reached, wear leveling maps writes of a logical block to a different physical block. This prevents a single physical block from prematurely failing due to a high concentration of writes. If wear leveling is improperly implemented, attackers may be able to programmatically cause the storage to become unreliable within a much shorter time than would normally be expected.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-212

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Instability — Notes:

## Potential Mitigations

**•** Architecture and Design: Include secure wear leveling algorithms and ensure they may not be bypassed. (Effectiveness: High)

## Applicable Platforms

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

## Demonstrative Examples

**•** Below is example code from [REF-1058] that the user can execute repeatedly to cause line failure. W is the maximum associativity of any cache in the system; S is the size of the largest cache in the system.