# CWE Detail – CWE-1248

## Description

The security-sensitive hardware module contains semiconductor defects.

## Extended Description

A semiconductor device can fail for various reasons. While some are manufacturing and packaging defects, the rest are due to prolonged use or usage under extreme conditions. Some mechanisms that lead to semiconductor defects include encapsulation failure, die-attach failure, wire-bond failure, bulk-silicon defects, oxide-layer faults, aluminum-metal faults (including electromigration, corrosion of aluminum, etc.), and thermal/electrical stress. These defects manifest as faults on chip-internal signals or registers, have the effect of inputs, outputs, or intermediate signals being always 0 or always 1, and do not switch as expected. If such faults occur in security-sensitive hardware modules, the security objectives of the hardware module may be compromised.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-624
* CAPEC-625

## Modes of Introduction

**•** Manufacturing: May be introduced due to issues in the manufacturing environment or improper handling of components, for example.

**•** Operation: May be introduced by improper handling or usage outside of rated operating environments (temperature, humidity, etc.)

## Common Consequences

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

## Potential Mitigations

**•** Testing: While semiconductor-manufacturing companies implement several mechanisms to continuously improve the semiconductor manufacturing process to ensure reduction of defects, some defects can only be fixed after manufacturing. Post-manufacturing testing of silicon die is critical. Fault models such as stuck-at-0 or stuck-at-1 must be used to develop post-manufacturing test cases and achieve good coverage. Once the silicon packaging is done, extensive post-silicon testing must be performed to ensure that hardware logic implementing security functionalities is defect-free. (Effectiveness: N/A)

**•** Operation: Operating the hardware outside device specification, such as at extremely high temperatures, voltage, etc., accelerates semiconductor degradation and results in defects. When these defects manifest as faults in security-critical, hardware modules, it results in compromise of security guarantees. Thus, operating the device within the specification is important. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Post-manufacture testing must be performed to ensure that hardware logic implementing security functionalities is defect-free.