# CWE Detail – CWE-1351

## Description

A hardware device, or the firmware running on it, is
 missing or has incorrect protection features to maintain
 goals of security primitives when the device is cooled below
 standard operating temperatures.

## Extended Description

The hardware designer may improperly anticipate
 hardware behavior when exposed to exceptionally cold
 conditions. As a result they may introduce a weakness by not
 accounting for the modified behavior of critical components
 when in extreme environments. An example of a change in behavior is that power loss
 won't clear/reset any volatile state when cooled below
 standard operating temperatures. This may result in
 a weakness when the starting state of the volatile memory is
 being relied upon for a security decision. For example, a
 Physical Unclonable Function (PUF) may be supplied as a
 security primitive to improve confidentiality,
 authenticity, and integrity guarantees. However, when the
 PUF is paired with DRAM, SRAM, or another temperature
 sensitive entropy source, the system designer may introduce
 weakness by failing to account for the chosen entropy
 source's behavior at exceptionally low temperatures. In the
 case of DRAM and SRAM, when power is cycled at low
 temperatures, the device will not contain the bitwise
 biasing caused by inconsistencies in manufacturing and will
 instead contain the data from previous boot. Should the PUF
 primitive be used in a cryptographic construction which
 does not account for full adversary control of PUF seed
 data, weakness would arise. This weakness does not cover "Cold Boot Attacks"
 wherein RAM or other external storage is super cooled and
 read externally by an attacker.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-624
* CAPEC-625

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context, Unexpected State — Notes: Consequences of this weakness are highly contextual.

## Potential Mitigations

**•** Architecture and Design: The system should account for security primitive behavior when cooled outside standard temperatures. (Effectiveness: N/A)

## Applicable Platforms

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