# CWE Detail – CWE-1384

## Description

The product does not properly handle unexpected physical or environmental conditions that occur naturally or are artificially induced.

## Extended Description

Hardware products are typically only guaranteed to behave correctly within certain physical limits or environmental conditions. Such products cannot necessarily control the physical or external conditions to which they are subjected. However, the inability to handle such conditions can undermine a product's security. For example, an unexpected physical or environmental condition may cause the flipping of a bit that is used for an authentication decision. This unexpected condition could occur naturally or be induced artificially by an adversary. Physical or environmental conditions of concern are: Atmospheric characteristics: extreme temperature ranges, etc. Interference: electromagnetic interference (EMI), radio frequency interference (RFI), etc. Assorted light sources: white light, ultra-violet light (UV), lasers, infrared (IR), etc. Power variances: under-voltages, over-voltages, under-current, over-current, etc. Clock variances: glitching, overclocking, clock stretching, etc. Component aging and degradation Materials manipulation: focused ion beams (FIB), etc. Exposure to radiation: x-rays, cosmic radiation, etc.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2019-17391: Lack of anti-glitch protections allows an attacker to launch a physical attack to bypass the secure boot and read protected eFuses.

## Modes of Introduction

**•** Architecture and Design: The product's design might not consider checking and handling extreme conditions.

**•** Manufacturing: For hardware manufacturing, sub-par components might be chosen that are not able to handle the expected environmental conditions.

## Common Consequences

**•** Impact: Varies by Context, Unexpected State — Notes: Consequences of this weakness are highly dependent on the role of affected components within the larger product.

## Potential Mitigations

**•** Requirements: In requirements, be specific about expectations for how the product will perform when it exceeds physical and environmental boundary conditions, e.g., by shutting down. (Effectiveness: N/A)

**•** Architecture and Design: Where possible, include independent components that can detect excess environmental conditions and have the capability to shut down the product. (Effectiveness: N/A)

**•** Architecture and Design: Where possible, use shielding or other materials that can increase the adversary's workload and reduce the likelihood of being able to successfully trigger a security-related failure. (Effectiveness: N/A)