# CWE Detail – CWE-1247

## Description

The device does not contain or contains incorrectly implemented circuitry or sensors to detect and mitigate voltage and clock glitches and protect sensitive information or software contained on the device.

## Extended Description

A device might support features such as secure boot which are supplemented with hardware and firmware support. This involves establishing a chain of trust, starting with an immutable root of trust by checking the signature of the next stage (culminating with the OS and runtime software) against a golden value before transferring control. The intermediate stages typically set up the system in a secure state by configuring several access control settings. Similarly, security logic for exercising a debug or testing interface may be implemented in hardware, firmware, or both. A device needs to guard against fault attacks such as voltage glitches and clock glitches that an attacker may employ in an attempt to compromise the system.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## 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.

**•** CVE-2021-33478: IP communication firmware allows access to a boot shell via certain impulses

## Related Attack Patterns (CAPEC)

* CAPEC-624
* CAPEC-625

## Modes of Introduction

**•** Operation: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Bypass Protection Mechanism, Read Memory, Modify Memory, Execute Unauthorized Code or Commands — Notes:

## Potential Mitigations

**•** Architecture and Design: At the circuit-level, using Tunable Replica Circuits (TRCs) or special flip-flops such as Razor flip-flops helps mitigate glitch attacks. Working at the SoC or platform base, level sensors may be implemented to detect glitches. Implementing redundancy in security-sensitive code (e.g., where checks are performed)also can help with mitigation of glitch attacks. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** After bypassing secure boot, an attacker can gain access to system assets to which the attacker should not have access.