# CWE Detail – CWE-1256

## Description

The product provides software-controllable
 device functionality for capabilities such as power and
 clock management, but it does not properly limit
 functionality that can lead to modification of
 hardware memory or register bits, or the ability to
 observe physical side channels.

## Extended Description

It is frequently assumed that physical attacks
 such as fault injection and side-channel analysis
 require an attacker to have physical access to the
 target device. This assumption may be false if the
 device has improperly secured power management features,
 or similar features. For mobile devices, minimizing
 power consumption is critical, but these devices run a
 wide variety of applications with different performance
 requirements. Software-controllable mechanisms to
 dynamically scale device voltage and frequency and
 monitor power consumption are common features in today's
 chipsets, but they also enable attackers to mount fault
 injection and side-channel attacks without having
 physical access to the device. Fault injection attacks involve strategic
 manipulation of bits in a device to achieve a desired
 effect such as skipping an authentication step,
 elevating privileges, or altering the output of a
 cryptographic operation. Manipulation of the device
 clock and voltage supply is a well-known technique to
 inject faults and is cheap to implement with physical
 device access. Poorly protected power management
 features allow these attacks to be performed from
 software. Other features, such as the ability to write
 repeatedly to DRAM at a rapid rate from unprivileged
 software, can result in bit flips in other memory
 locations (Rowhammer, [REF-1083]). Side channel analysis requires gathering
 measurement traces of physical quantities such as power
 consumption. Modern processors often include power
 metering capabilities in the hardware itself (e.g.,
 Intel RAPL) which if not adequately protected enable
 attackers to gather measurements necessary for
 performing side-channel attacks from software.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2019-11157: Plundervolt: Improper conditions check in voltage settings for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege and/or information disclosure via local access [REF-1081].

**•** CVE-2020-8694: PLATYPUS Attack: Insufficient access control in the Linux kernel driver for some Intel processors allows information disclosure.

**•** CVE-2020-8695: Observable discrepancy in the RAPL interface for some Intel processors allows information disclosure.

**•** CVE-2020-12912: AMD extension to a Linux service does not require privileged access to the RAPL interface, allowing side-channel attacks.

**•** CVE-2015-0565: NaCl in 2015 allowed the CLFLUSH instruction, making Rowhammer attacks possible.

## Related Attack Patterns (CAPEC)

* CAPEC-624
* CAPEC-625

## Modes of Introduction

**•** Architecture and Design: An architect may initiate introduction of
 this weakness via exacting requirements for
 software accessible power/clock management
 requirements

**•** Implementation: An implementer may introduce this weakness
 by assuming there are no consequences to unbounded
 power and clock management for secure components
 from untrusted ones.

## Common Consequences

**•** Impact: Modify Memory, Modify Application Data, Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Ensure proper access control mechanisms protect software-controllable features altering physical operating conditions such as clock frequency and voltage. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Preventing the loop required to defeat the Rowhammer exploit is not always possible:

**•** N/A

**•** We assume that untrusted software running on any of the
 Core{0-N} processors has access to the input and output
 ports of the hrot\_iface. If untrusted software can clear
 the lock\_bit or write the clock frequency and voltage
 registers due to inadequate protection, a fault
 injection attack could be performed.