# CWE Detail – CWE-1320

## Description

Untrusted agents can disable alerts about signal conditions exceeding limits or the response mechanism that handles such alerts.

## Extended Description

Hardware sensors are used to detect whether a device is operating within design limits. The threshold values for these limits are set by hardware fuses or trusted software such as a BIOS.   
 Modification of these limits may be protected by hardware mechanisms. When device sensors detect out of bound conditions, alert signals may be generated for remedial action, which may take the form of device shutdown or throttling. Warning signals that are not properly secured may be disabled or used to generate spurious alerts, causing degraded performance or denial-of-service (DoS).  
 These alerts may be masked by untrusted software. Examples of these alerts involve thermal and power sensor alerts.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-1
* CAPEC-180

## Attack TTPs

**•** T1574.010: Services File Permissions Weakness (Tactics: persistence, privilege-escalation, defense-evasion)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: DoS: Instability, DoS: Crash, Exit, or Restart, Reduce Reliability, Unexpected State — Notes:

## Potential Mitigations

**•** Architecture and Design: Alert signals generated by critical events should be protected from access by untrusted agents. Only hardware or trusted firmware modules should be able to alter the alert configuration. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Reprogramming the state of the GPIO pin allows malicious software to trigger spurious alerts or to set the alert pin to a zero value so that thermal sensor alerts are not received by the processor.