# CWE Detail – CWE-1224

## Description

The hardware design control register "sticky bits" or write-once bit fields are improperly implemented, such that they can be reprogrammed by software.

## Extended Description

Integrated circuits and hardware IP software programmable controls and settings are commonly stored in register circuits. These register contents have to be initialized at hardware reset to define default values that are hard coded in the hardware description language (HDL) code of the hardware unit. A common security protection method used to protect register settings from modification by software is to make the settings write-once or "sticky." This allows writing to such registers only once, whereupon they become read-only. This is useful to allow initial boot software to configure systems settings to secure values while blocking runtime software from modifying such hardware settings. Failure to implement write-once restrictions in hardware design can expose such registers to being re-programmed by software and written multiple times. For example, write-once fields could be implemented to only be write-protected if they have been set to value "1", wherein they would work as "write-1-once" and not "write-once".

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-680

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: Such issues could be introduced during implementation of hardware design, since IP parameters and defaults are defined in HDL code and identified later during Testing or System Configuration phases.

## Common Consequences

**•** Impact: Varies by Context — Notes: System configuration cannot be programmed in a secure way.

## Potential Mitigations

**•** Architecture and Design: During hardware design all register write-once or sticky fields must be evaluated for proper configuration. (Effectiveness: N/A)

**•** Testing: The testing phase should use automated tools to test that values are not reprogrammable and that write-once fields lock on writing zeros. (Effectiveness: N/A)

## Applicable Platforms

**•** Verilog (Class: None, Prevalence: Undetermined)

**•** VHDL (Class: None, Prevalence: Undetermined)

## Demonstrative Examples

**•** The above example only locks further writes if write\_once\_status bit is written to one. So it acts as write\_1-Once instead of the write-once attribute.