# CWE Detail – CWE-1269

## Description

The product released to market is released in pre-production or manufacturing configuration.

## Extended Description

Products in the pre-production or manufacturing stages are configured to have many debug hooks and debug capabilities, including but not limited to: Ability to override/bypass various cryptographic checks (including authentication, authorization, and integrity) Ability to read/write/modify/dump internal state (including registers and memory) Ability to change system configurations Ability to run hidden or private commands that are not allowed during production (as they expose IP). The above is by no means an exhaustive list, but it alludes to the greater capability and the greater state of vulnerability of a product during it's preproduction or manufacturing state. Complexity increases when multiple parties are involved in executing the tests before the final production version. For example, a chipmaker might fabricate a chip and run its own preproduction tests, following which the chip would be delivered to the Original Equipment Manufacturer (OEM), who would now run a second set of different preproduction tests on the same chip. Only after both of these sets of activities are complete, can the overall manufacturing phase be called "complete" and have the "Manufacturing Complete" fuse blown. However, if the OEM forgets to blow the Manufacturing Complete fuse, then the system remains in the manufacturing stage, rendering the system both exposed and vulnerable.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2019-13945: Regarding SSA-686531, a hardware based manufacturing access on S7-1200 and  
S7-200 SMART has occurred. A vulnerability has been identified in SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-200 SMART CPU family (All versions). There is an access mode used during manufacturing of S7-1200 CPUs that allows additional diagnostic functionality. The security vulnerability could be exploited by an attacker with physical access to the UART interface during boot process. At the time of advisory publication, no public exploitation of this security vulnerability was known.

**•** CVE-2018-4251: Laptops with Intel chipsets were found to be running in Manufacturing Mode. After this information was reported to the OEM, the vulnerability (CVE-2018-4251) was patched disallowing access to the interface.

## Related Attack Patterns (CAPEC)

* CAPEC-439

## Attack TTPs

**•** T1195: Supply Chain Compromise (Tactics: initial-access)

## Modes of Introduction

**•** Implementation: N/A

**•** Integration: N/A

**•** Manufacturing: N/A

## Common Consequences

**•** Impact: Other — Notes:

## Potential Mitigations

**•** Implementation: Ensure that there exists a marker for denoting the Manufacturing Complete stage and that the Manufacturing Complete marker gets updated at the Manufacturing Complete stage (i.e., the Manufacturing Complete fuse gets blown). (Effectiveness: N/A)

**•** Integration: Ensure that there exists a marker for denoting the Manufacturing Complete stage and that the Manufacturing Complete marker gets updated at the Manufacturing Complete stage (i.e., the Manufacturing Complete fuse gets blown). (Effectiveness: N/A)

**•** Manufacturing: Ensure that there exists a marker for denoting the Manufacturing Complete stage and that the Manufacturing Complete marker gets updated at the Manufacturing Complete stage (i.e., the Manufacturing Complete fuse gets blown). (Effectiveness: N/A)

## Applicable Platforms

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

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

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

## Demonstrative Examples

**•** An attacker will now be able to scan all the internal memory (containing chipmaker-level secrets).