# CWE Detail – CWE-1297

## Description

The product does not adequately protect confidential information on the device from being accessed by Outsourced Semiconductor Assembly and Test (OSAT) vendors.

## Extended Description

In contrast to complete vertical integration of architecting, designing, manufacturing, assembling, and testing chips all within a single organization, an organization can choose to simply architect and design a chip before outsourcing the rest of the process to OSAT entities (e.g., external foundries and test houses). In the latter example, the device enters an OSAT facility in a much more vulnerable pre-production stage where many debug and test modes are accessible. Therefore, the chipmaker must place a certain level of trust with the OSAT. To counter this, the chipmaker often requires the OSAT partner to enter into restrictive non-disclosure agreements (NDAs). Nonetheless, OSAT vendors likely have many customers, which increases the risk of accidental sharing of information. There may also be a security vulnerability in the information technology (IT) system of the OSAT facility. Alternatively, a malicious insider at the OSAT facility may carry out an insider attack. Considering these factors, it behooves the chipmaker to minimize any confidential information in the device that may be accessible to the OSAT vendor. Logic errors during design or synthesis could misconfigure the interconnection of the debug components, which could provide improper authorization to sensitive information.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## 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

**•** Implementation: N/A

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Bypass Protection Mechanism, Execute Unauthorized Code or Commands, Modify Memory, Modify Files or Directories — Notes: The impact depends on the confidential information itself and who is inadvertently granted access. For example, if the confidential information is a key that can unlock all the parts of a generation, the impact could be severe.

## Potential Mitigations

**•** Architecture and Design: Ensure that when an OSAT vendor is allowed to access test interfaces necessary for preproduction and returned parts, the vendor only pulls the minimal information necessary. Also, architect the product in such a way that, when an "unlock device" request comes, it only unlocks that specific part and not all the parts for that product line. Ensure that the product's non-volatile memory (NVM) is scrubbed of all confidential information and secrets before handing it over to an OSAT. Arrange to secure all communication between an OSAT facility and the chipmaker. (Effectiveness: Moderate)

## Applicable Platforms

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

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

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

## Demonstrative Examples

**•** Suppose the preproduction device contains NVM (a storage medium that by definition/design can retain its data without power), and this NVM contains a key that can unlock all the parts for that generation. An OSAT facility accidentally leaks the key.

## Notes

**•** Maintenance: This entry might be subject to CWE Scope Exclusion SCOPE.SITUATIONS (Focus on situations in which weaknesses may appear); SCOPE.HUMANPROC (Human/organizational process; and/or SCOPE.CUSTREL (Not customer-relevant).

**•** Maintenance: This entry is still under development and will continue to see updates and content improvements.