# CWE Detail – CWE-1296

## Description

The product's debug components contain incorrect chaining or granularity of debug components.

## Extended Description

For debugging and troubleshooting a chip, several hardware design elements are often implemented, including: Various Test Access Ports (TAPs) allow boundary scan commands to be executed. For scanning the internal components of a chip, there are scan cells that allow the chip to be used as a "stimulus and response" mechanism. Chipmakers might create custom methods to observe the internal components of their chips by placing various tracing hubs within their chip and creating hierarchical or interconnected structures among those hubs. Logic errors during design or synthesis could misconfigure the interconnection of the debug components, which could allow unintended access permissions.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2017-18347: Incorrect access control in RDP Level 1 on STMicroelectronics STM32F0 series devices allows physically present attackers to extract the device's protected firmware via a special sequence of Serial Wire Debug (SWD) commands because there is a race condition between full initialization of the SWD interface and the setup of flash protection.

**•** CVE-2020-1791: There is an improper authorization vulnerability in several smartphones. The system has a logic-judging error, and, under certain scenarios, a successful exploit could allow the attacker to switch to third desktop after a series of operations in ADB mode. (Vulnerability ID: HWPSIRT-2019-10114).

## Related Attack Patterns (CAPEC)

* CAPEC-121
* CAPEC-702

## 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: Depending on the access to debug component(s) erroneously granted, an attacker could use the debug component to gain additional understanding about the system to further an attack and/or execute other commands. This could compromise any security property, including the ones listed above.

## Potential Mitigations

**•** Implementation: Ensure that debug components are properly chained and their granularity is maintained at different authentication levels. (Effectiveness: N/A)

## Applicable Platforms

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

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

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

## Demonstrative Examples

**•** In a System-on-Chip (SoC), the user might be able to access the SoC-level TAP with a certain level of authorization. However, this access should not also grant access to all of the internal TAPs (e.g., Core). Separately, if any of the internal TAPs is also stitched to the TAP chain when it should not be because of a logic error, then an attacker can access the internal TAPs as well and execute commands there.

## Notes

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