# CWE Detail – CWE-1295

## Description

The product fails to adequately prevent the revealing of unnecessary and potentially sensitive system information within debugging messages.

## Extended Description

Debug messages are messages that help troubleshoot an issue by revealing the internal state of the system. For example, debug data in design can be exposed through internal memory array dumps or boot logs through interfaces like UART via TAP commands, scan chain, etc. Thus, the more information contained in a debug message, the easier it is to debug. However, there is also the risk of revealing information that could help an attacker either decipher a vulnerability, and/or gain a better understanding of the system. Thus, this extra information could lower the "security by obscurity" factor. While "security by obscurity" alone is insufficient, it can help as a part of "Defense-in-depth".

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2021-25476: Digital Rights Management (DRM) capability for mobile platform leaks pointer information, simplifying ASLR bypass

**•** CVE-2020-24491: Processor generates debug message that contains sensitive information ("addresses of memory transactions").

**•** CVE-2017-18326: modem debug messages include cryptographic keys

## Related Attack Patterns (CAPEC)

* CAPEC-121

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Memory, Bypass Protection Mechanism, Gain Privileges or Assume Identity, Varies by Context — Notes:

## Potential Mitigations

**•** Implementation: Ensure that a debug message does not reveal any unnecessary information during the debug process for the intended response. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Example 1: Suppose in response to a Test Access Port (TAP) chaining request the debug message also reveals the current TAP hierarchy (the full topology) in addition to the success/failure message.