# CWE Detail – CWE-1258

## Description

The hardware does not fully clear security-sensitive values, such as keys and intermediate values in cryptographic operations, when debug mode is entered.

## Extended Description

Security sensitive values, keys, intermediate steps of cryptographic operations, etc. are stored in temporary registers in the hardware. If these values are not cleared when debug mode is entered they may be accessed by a debugger allowing sensitive information to be accessible by untrusted parties.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2021-33080: Uncleared debug information in memory accelerator for SSD product exposes sensitive system information

**•** CVE-2022-31162: Rust library leaks Oauth client details in application debug logs

## Related Attack Patterns (CAPEC)

* CAPEC-150
* CAPEC-204
* CAPEC-37
* CAPEC-545

## Attack TTPs

**•** T1003: OS Credential Dumping (Tactics: credential-access)

**•** T1602: Data from Configuration Repository (Tactics: collection)

**•** T1555.001: Keychain (Tactics: credential-access)

**•** T1119: Automated Collection (Tactics: collection)

**•** T1530: Data from Cloud Storage (Tactics: collection)

**•** T1005: Data from Local System (Tactics: collection)

**•** T1555: Credentials from Password Stores (Tactics: credential-access)

**•** T1552.004: Private Keys (Tactics: credential-access)

**•** T1213: Data from Information Repositories (Tactics: collection)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Memory — Notes:

**•** Impact: Bypass Protection Mechanism — Notes:

## Potential Mitigations

**•** Architecture and Design: Whenever debug mode is enabled, all registers containing sensitive assets must be cleared. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

**•** To address the issue, it is essential to ensure that the register is cleared and zeroized after activating debug mode on the SoC. In the correct implementation illustrated in the good code below, core\_keyx registers are set to zero when debug mode is activated [REF-1436].