# CWE Detail – CWE-1301

## Description

The product's data removal process does not completely delete all data and potentially sensitive information within hardware components.

## Extended Description

Physical properties of hardware devices, such as remanence of magnetic media, residual charge of ROMs/RAMs, or screen burn-in may still retain sensitive data after a data removal process has taken place and power is removed. Recovering data after erasure or overwriting is possible due to a phenomenon called data remanence. For example, if the same value is written repeatedly to a memory location, the corresponding memory cells can become physically altered to a degree such that even after the original data is erased that data can still be recovered through physical characterization of the memory cells.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2019-8575: Firmware Data Deletion Vulnerability in which a base station factory reset might not delete all user information. The impact of this enables a new owner of a used device that has been "factory-default reset" with a vulnerable firmware version can still retrieve, at least, the previous owner's wireless network name, and the previous owner's wireless security (such as WPA2) key. This issue was addressed with improved, data deletion.

## Related Attack Patterns (CAPEC)

* CAPEC-37

## Attack TTPs

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

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

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Memory, Read Application Data — Notes:

## Potential Mitigations

**•** Architecture and Design: Apply blinding or masking techniques to implementations of cryptographic algorithms. (Effectiveness: N/A)

**•** Implementation: Alter the method of erasure, add protection of media, or destroy the media to protect the data. (Effectiveness: N/A)

## Applicable Platforms

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

## Notes

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