# CWE Detail – CWE-1330

## Description

Confidential information stored in memory circuits is readable or recoverable after being cleared or erased.

## Extended Description

Data remanence occurs when stored, memory content is not fully lost after a memory-clear or -erase operation. Confidential memory contents can still be readable through data remanence in the hardware. Data remanence can occur because of performance optimization or memory organization during 'clear' or 'erase' operations, like a design that allows the memory-organization metadata (e.g., file pointers) to be erased without erasing the actual memory content. To protect against this weakness, memory devices will often support different commands for optimized memory erase and explicit secure erase. Data remanence can also happen because of the physical properties of memory circuits in use. For example, static, random-access-memory (SRAM) and dynamic, random-access-memory (DRAM) data retention is based on the charge retained in the memory cell, which depends on factors such as power supply, refresh rates, and temperature. Other than explicit erase commands, self-encrypting, secure-memory devices can also support secure erase through cryptographic erase commands. In such designs, only the decryption keys for encrypted data stored on the device are erased. That is, the stored data are always remnant in the media after a cryptographic erase. However, only the encrypted data can be extracted. Thus, protection against data recovery in such designs relies on the strength of the encryption algorithm.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## 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-150
* 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: Modify Memory, Read Memory — Notes: Confidential data are readable to untrusted agent.

## Potential Mitigations

**•** Architecture and Design: Support for secure-erase commands that apply multiple cycles of overwriting memory with known patterns and of erasing actual content. Support for cryptographic erase in self-encrypting, memory devices. External, physical tools to erase memory such as ultraviolet-rays-based erase of Electrically erasable, programmable, read-only memory (EEPROM). Physical destruction of media device. This is done for repurposed or scrapped devices that are no longer in use. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The device also supports user reset to factory defaults with the expectation that all personal information is erased from the device after this operation. On factory reset, user files are erased using explicit, erase commands supported by the flash device.