# CWE Detail – CWE-1266

## Description

The product does not properly provide a capability for the product administrator to remove sensitive data at the time the product is decommissioned. A scrubbing capability could be missing, insufficient, or incorrect.

## Extended Description

When a product is decommissioned - i.e., taken out of service - best practices or regulatory requirements may require the administrator to remove or overwrite sensitive data first, i.e. "scrubbing." Improper scrubbing of sensitive data from a decommissioned device leaves that data vulnerable to acquisition by a malicious actor. Sensitive data may include, but is not limited to, device/manufacturer proprietary information, user/device credentials, network configurations, and other forms of sensitive data.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-150
* CAPEC-37
* CAPEC-545
* CAPEC-546
* CAPEC-675

## 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)

**•** T1052: Exfiltration Over Physical Medium (Tactics: exfiltration)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Policy: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Memory — Notes:

## Potential Mitigations

**•** Architecture and Design: Functionality to completely scrub data from a product at the conclusion of its lifecycle should be part of the design phase. Trying to add this function on top of an existing architecture could lead to incomplete removal of sensitive information/data. (Effectiveness: N/A)

**•** Policy: The manufacturer should describe the location(s) where sensitive data is stored and the policies and procedures for its removal. This information may be conveyed, for example, in an Administrators Guide or a Statement of Volatility. (Effectiveness: N/A)

**•** Implementation: If the capability to wipe sensitive data isn't built-in, the manufacturer may need to provide a utility to scrub sensitive data from storage if that data is located in a place which is non-accessible by the administrator. One example of this could be when sensitive data is stored on an EEPROM for which there is no user/admin interface provided by the system. (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.