# CWE Detail – CWE-459

## Description

The product does not properly "clean up" and remove temporary or supporting resources after they have been used.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2000-0552: World-readable temporary file not deleted after use.

**•** CVE-2005-2293: Temporary file not deleted after use, leaking database usernames and passwords.

**•** CVE-2002-0788: Interaction error creates a temporary file that can not be deleted due to strong permissions.

**•** CVE-2002-2066: Alternate data streams for NTFS files are not cleared when files are wiped (alternate channel / infoleak).

**•** CVE-2002-2067: Alternate data streams for NTFS files are not cleared when files are wiped (alternate channel / infoleak).

**•** CVE-2002-2068: Alternate data streams for NTFS files are not cleared when files are wiped (alternate channel / infoleak).

**•** CVE-2002-2069: Alternate data streams for NTFS files are not cleared when files are wiped (alternate channel / infoleak).

**•** CVE-2002-2070: Alternate data streams for NTFS files are not cleared when files are wiped (alternate channel / infoleak).

**•** CVE-2005-1744: Users not logged out when application is restarted after security-relevant changes were made.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Other, Read Application Data, Modify Application Data, DoS: Resource Consumption (Other) — Notes: It is possible to overflow the number of temporary files because directories typically have limits on the number of files allowed. This could create a denial of service problem.

## Potential Mitigations

**•** Architecture and Design: Temporary files and other supporting resources should be deleted/released immediately after they are no longer needed. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** N/A

## Notes

**•** Relationship: CWE-459 is a child of CWE-404 because, while CWE-404 covers any type of improper shutdown or release of a resource, CWE-459 deals specifically with a multi-step shutdown process in which a crucial step for "proper" cleanup is omitted or impossible. That is, CWE-459 deals specifically with a cleanup or shutdown process that does not successfully remove all potentially sensitive data.

**•** Relationship: Overlaps other categories such as permissions and containment. Concept needs further development. This could be primary (e.g. leading to infoleak) or resultant (e.g. resulting from unhandled error conditions or early termination).