# CWE Detail – CWE-403

## Description

A process does not close sensitive file descriptors before invoking a child process, which allows the child to perform unauthorized I/O operations using those descriptors.

## Extended Description

When a new process is forked or executed, the child process inherits any open file descriptors. When the child process has fewer privileges than the parent process, this might introduce a vulnerability if the child process can access the file descriptor but does not have the privileges to access the associated file.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2003-0740: Server leaks a privileged file descriptor, allowing the server to be hijacked.

**•** CVE-2004-1033: File descriptor leak allows read of restricted files.

**•** CVE-2000-0094: Access to restricted resource using modified file descriptor for stderr.

**•** CVE-2002-0638: Open file descriptor used as alternate channel in complex race condition.

**•** CVE-2003-0489: Program does not fully drop privileges after creating a file descriptor, which allows access to the descriptor via a separate vulnerability.

**•** CVE-2003-0937: User bypasses restrictions by obtaining a file descriptor then calling setuid program, which does not close the descriptor.

**•** CVE-2004-2215: Terminal manager does not properly close file descriptors, allowing attackers to access terminals of other users.

**•** CVE-2006-5397: Module opens a file for reading twice, allowing attackers to read files.

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

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

## Applicable Platforms

**•** C (Class: None, Prevalence: Undetermined)

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