# CWE Detail – CWE-69

## Description

The product does not properly prevent access to, or detect usage of, alternate data streams (ADS).

## Extended Description

An attacker can use an ADS to hide information about a file (e.g. size, the name of the process) from a system or file browser tools such as Windows Explorer and 'dir' at the command line utility. Alternately, the attacker might be able to bypass intended access restrictions for the associated data fork.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-1999-0278: In IIS, remote attackers can obtain source code for ASP files by appending "::$DATA" to the URL.

**•** CVE-2000-0927: Product does not properly record file sizes if they are stored in alternative data streams, which allows users to bypass quota restrictions.

## Related Attack Patterns (CAPEC)

* CAPEC-168

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Hide Activities, Other — Notes:

## Potential Mitigations

**•** Testing: Software tools are capable of finding ADSs on your system. (Effectiveness: N/A)

**•** Implementation: Ensure that the source code correctly parses the filename to read or write to the correct stream. (Effectiveness: N/A)

## Applicable Platforms

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

## Notes

**•** Theoretical: This and similar problems exist because the same resource can have multiple identifiers that dictate which behavior can be performed on the resource.