# CWE Detail – CWE-48

## Description

The product accepts path input in the form of internal space ('file(SPACE)name') without appropriate validation, which can lead to ambiguous path resolution and allow an attacker to traverse the file system to unintended locations or access arbitrary files.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2000-0293: Filenames with spaces allow arbitrary file deletion when the product does not properly quote them; some overlap with path traversal.

**•** CVE-2001-1567: "+" characters in query string converted to spaces before sensitive file/extension (internal space), leading to bypass of access restrictions to the file.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Files or Directories, Modify Files or Directories — Notes:

## Applicable Platforms

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

## Notes

**•** Relationship: This weakness is likely to overlap quoting problems, e.g. the "Program Files" unquoted search path (CWE-428). It also could be an equivalence issue if filtering removes all extraneous spaces.

**•** Relationship: Whitespace can be a factor in other weaknesses not directly related to equivalence. It can also be used to spoof icons or hide files with dangerous names (see icon manipulation and visual truncation in CWE-451).