# CWE Detail – CWE-46

## Description

The product accepts path input in the form of trailing space ('filedir ') 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-2001-0693: Source disclosure via trailing encoded space "%20"

**•** CVE-2001-0778: Source disclosure via trailing encoded space "%20"

**•** CVE-2001-1248: Source disclosure via trailing encoded space "%20"

**•** CVE-2004-0280: Source disclosure via trailing encoded space "%20"

**•** CVE-2004-2213: Source disclosure via trailing encoded space "%20"

**•** CVE-2005-0622: Source disclosure via trailing encoded space "%20"

**•** CVE-2005-1656: Source disclosure via trailing encoded space "%20"

**•** CVE-2002-1603: Source disclosure via trailing encoded space "%20"

**•** CVE-2001-0054: Multi-Factor Vulnerability (MFV). directory traversal and other issues in FTP server using Web encodings such as "%20"; certain manipulations have unusual side effects.

**•** CVE-2002-1451: Trailing space ("+" in query string) leads to source code disclosure.

## Related Attack Patterns (CAPEC)

* CAPEC-649

## Attack TTPs

**•** T1036.006: Space after Filename (Tactics: defense-evasion)

## 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)