# CWE Detail – CWE-49

## Description

The product accepts path input in the form of trailing slash ('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-2002-0253: Overlaps infoleak

**•** CVE-2001-0446: Application server allows remote attackers to read source code for .jsp files by appending a / to the requested URL.

**•** CVE-2004-0334: Bypass Basic Authentication for files using trailing "/"

**•** CVE-2001-0893: Read sensitive files with trailing "/"

**•** CVE-2001-0892: Web server allows remote attackers to view sensitive files under the document root (such as .htpasswd) via a GET request with a trailing /.

**•** CVE-2004-1814: Directory traversal vulnerability in server allows remote attackers to read protected files via .. (dot dot) sequences in an HTTP request.

## Modes of Introduction

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

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

## Applicable Platforms

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