# CWE Detail – CWE-50

## Description

The product accepts path input in the form of multiple leading slash ('//multiple/leading/slash') 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-2002-1483: Read files with full pathname using multiple internal slash.

**•** CVE-1999-1456: Server allows remote attackers to read arbitrary files via a GET request with more than one leading / (slash) character in the filename.

**•** CVE-2004-0578: Server allows remote attackers to read arbitrary files via leading slash (//) characters in a URL request.

**•** CVE-2002-0275: Server allows remote attackers to bypass authentication and read restricted files via an extra / (slash) in the requested URL.

**•** CVE-2004-1032: Product allows local users to delete arbitrary files or create arbitrary empty files via a target filename with a large number of leading slash (/) characters.

**•** CVE-2002-1238: Server allows remote attackers to bypass access restrictions for files via an HTTP request with a sequence of multiple / (slash) characters such as http://www.example.com///file/.

**•** CVE-2004-1878: Product allows remote attackers to bypass authentication, obtain sensitive information, or gain access via a direct request to admin/user.pl preceded by // (double leading slash).

**•** CVE-2005-1365: Server allows remote attackers to execute arbitrary commands via a URL with multiple leading "/" (slash) characters and ".." sequences.

**•** CVE-2000-1050: Access directory using multiple leading slash.

**•** CVE-2001-1072: Bypass access restrictions via multiple leading slash, which causes a regular expression to fail.

**•** CVE-2004-0235: Archive extracts to arbitrary files using multiple leading slash in filenames in the archive.

## 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)