# CWE Detail – CWE-45

## Description

The product accepts path input in the form of multiple internal dot ('file...dir') 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

## 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: An improper attempt to remove the internal dots from the string could lead to CWE-181 (Incorrect Behavior Order: Validate Before Filter).