# CWE Detail – CWE-249

## Description

This entry has been deprecated because of name  
 confusion and an accidental combination of multiple  
 weaknesses. Most of its content has been transferred to  
 CWE-785.

## Extended Description

This entry was deprecated for several reasons. The primary  
 reason is over-loading of the "path manipulation" term and the  
 description. The original description for this entry was the  
 same as that for the "Often Misused: File System" item in the  
 original Seven Pernicious Kingdoms paper. However, Seven  
 Pernicious Kingdoms also has a "Path Manipulation" phrase that  
 is for external control of pathnames (CWE-73), which is a  
 factor in symbolic link following and path traversal, neither  
 of which is explicitly mentioned in 7PK. Fortify uses the  
 phrase "Often Misused: Path Manipulation" for a broader range  
 of problems, generally for issues related to buffer  
 management. Given the multiple conflicting uses of this term,  
 there is a chance that CWE users may have incorrectly mapped  
 to this entry. The second reason for deprecation is an implied combination of  
 multiple weaknesses within buffer-handling functions. The  
 focus of this entry was generally on the path-conversion  
 functions and their association with buffer  
 overflows. However, some of Fortify's Vulncat entries have the  
 term "path manipulation" but describe a non-overflow weakness  
 in which the buffer is not guaranteed to contain the entire  
 pathname, i.e., there is information truncation (see CWE-222  
 for a similar concept). A new entry for this non-overflow  
 weakness may be created in a future version of CWE.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified