# CWE Detail – CWE-76

## Description

The product correctly neutralizes certain special elements, but it improperly neutralizes equivalent special elements.

## Extended Description

The product may have a fixed list of special characters it believes is complete. However, there may be alternate encodings, or representations that also have the same meaning. For example, the product may filter out a leading slash (/) to prevent absolute path names, but does not account for a tilde (~) followed by a user name, which on some \*nix systems could be expanded to an absolute pathname. Alternately, the product might filter a dangerous "-e" command-line switch when calling an external program, but it might not account for "--exec" or other switches that have the same semantics.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Other — Notes:

## Potential Mitigations

**•** Requirements: Programming languages and supporting technologies might be chosen which are not subject to these issues. (Effectiveness: N/A)

**•** Implementation: Utilize an appropriate mix of allowlist and denylist parsing to filter equivalent special element syntax from all input. (Effectiveness: N/A)

## Applicable Platforms

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