# CWE Detail – CWE-224

## Description

The product records security-relevant information according to an alternate name of the affected entity, instead of the canonical name.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-0725: Attacker performs malicious actions on a hard link to a file, obscuring the real target file.

## Modes of Introduction

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

**•** Operation: N/A

## Common Consequences

**•** Impact: Hide Activities, Gain Privileges or Assume Identity — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** While the code logs a bad access attempt, it logs the user supplied name for the file, not the canonicalized file name. An attacker can obscure their target by giving the script the name of a link to the file they are attempting to access. Also note this code contains a race condition between the is\_link() and readlink() functions (CWE-363).