# CWE Detail – CWE-223

## Description

The product does not record or display information that would be important for identifying the source or nature of an attack, or determining if an action is safe.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-1999-1029: Login attempts are not recorded if the user disconnects before the maximum number of tries.

**•** CVE-2002-1839: Sender's IP address not recorded in outgoing e-mail.

**•** CVE-2000-0542: Failed authentication attempts are not recorded if later attempt succeeds.

## Modes of Introduction

**•** Architecture and Design: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Hide Activities — Notes: The source of an attack will be difficult or impossible to determine. This can allow attacks to the system to continue without notice.

## Applicable Platforms

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

## Demonstrative Examples

**•** This code only logs failed login attempts when a certain limit is reached. If an attacker knows this limit, they can stop their attack from being discovered by avoiding the limit.

**•** 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).