# CWE Detail – CWE-221

## Description

The product does not record, or improperly records, security-relevant information that leads to an incorrect decision or hampers later analysis.

## Extended Description

This can be resultant, e.g. a buffer overflow might trigger a crash before the product can log the event.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2004-2227: Web browser's filename selection dialog only shows the beginning portion of long filenames, which can trick users into launching executables with dangerous extensions.

**•** CVE-2003-0412: application server does not log complete URI of a long request (truncation).

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

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

**•** CVE-1999-1055: Product does not warn user when document contains certain dangerous functions or macros.

## Related Attack Patterns (CAPEC)

* CAPEC-81

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Hide Activities — Notes:

## 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.