# CWE Detail – CWE-210

## Description

The product identifies an error condition and creates its own diagnostic or error messages that contain sensitive information.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2005-1745: Infoleak of sensitive information in error message (physical access required).

## Modes of Introduction

**•** Architecture and Design: N/A

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

## Common Consequences

**•** Impact: Read Application Data — Notes:

## Potential Mitigations

**•** Implementation: Debugging information should not make its way into a production release. (Effectiveness: N/A)

**•** Implementation: Debugging information should not make its way into a production release. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** If this code is running on a server, such as a web application, then the person making the request should not know what the full pathname of the configuration directory is. By submitting a username that is not associated with a configuration file, an attacker could get this pathname from the error message. It could then be used to exploit path traversal, symbolic link following, or other problems that may exist elsewhere in the application.