# CWE Detail – CWE-215

## Description

The product inserts sensitive information into debugging code, which could expose this information if the debugging code is not disabled in production.

## Extended Description

When debugging, it may be necessary to report detailed information to the programmer. However, if the debugging code is not disabled when the product is operating in a production environment, then this sensitive information may be exposed to attackers.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2004-2268: Password exposed in debug information.

**•** CVE-2002-0918: CGI script includes sensitive information in debug messages when an error is triggered.

**•** CVE-2003-1078: FTP client with debug option enabled shows password to the screen.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

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

## Potential Mitigations

**•** Implementation: Do not leave debug statements that could be executed in the source code. Ensure that all debug information is eradicated before releasing the software. (Effectiveness: N/A)

**•** Architecture and Design: Compartmentalize the system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area. Ensure that appropriate compartmentalization is built into the system design, and the compartmentalization allows for and reinforces privilege separation functionality. Architects and designers should rely on the principle of least privilege to decide the appropriate time to use privileges and the time to drop privileges. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** The code writes sensitive debug information to the client browser if the "debugEnabled" flag is set to true .

## Notes

**•** Relationship: This overlaps other categories.