# CWE Detail – CWE-205

## Description

The product's behaviors indicate important differences that may be observed by unauthorized actors in a way that reveals (1) its internal state or decision process, or (2) differences from other products with equivalent functionality.

## Extended Description

Ideally, a product should provide as little information about its internal operations as possible. Otherwise, attackers could use knowledge of these internal operations to simplify or optimize their attack. In some cases, behavioral discrepancies can be used by attackers to form a side channel.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-0208: Product modifies TCP/IP stack and ICMP error messages in unusual ways that show the product is in use.

**•** CVE-2004-2252: Behavioral infoleak by responding to SYN-FIN packets.

## Related Attack Patterns (CAPEC)

* CAPEC-541
* CAPEC-580

## Attack TTPs

**•** T1082: System Information Discovery (Tactics: discovery)

**•** T1592.002: Software (Tactics: reconnaissance)

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data, Bypass Protection Mechanism — Notes:

## Applicable Platforms

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