# CWE Detail – CWE-204

## Description

The product provides different responses to incoming requests in a way that reveals internal state information to an unauthorized actor outside of the intended control sphere.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-2094: This, and others, use ".." attacks and monitor error responses, so there is overlap with directory traversal.

**•** CVE-2001-1483: Enumeration of valid usernames based on inconsistent responses

**•** CVE-2001-1528: Account number enumeration via inconsistent responses.

**•** CVE-2004-2150: User enumeration via discrepancies in error messages.

**•** CVE-2005-1650: User enumeration via discrepancies in error messages.

**•** CVE-2004-0294: Bulletin Board displays different error messages when a user exists or not, which makes it easier for remote attackers to identify valid users and conduct a brute force password guessing attack.

**•** CVE-2004-0243: Operating System, when direct remote login is disabled, displays a different message if the password is correct, which allows remote attackers to guess the password via brute force methods.

**•** CVE-2002-0514: Product allows remote attackers to determine if a port is being filtered because the response packet TTL is different than the default TTL.

**•** CVE-2002-0515: Product sets a different TTL when a port is being filtered than when it is not being filtered, which allows remote attackers to identify filtered ports by comparing TTLs.

**•** CVE-2001-1387: Product may generate different responses than specified by the administrator, possibly leading to an information leak.

**•** CVE-2004-0778: Version control system allows remote attackers to determine the existence of arbitrary files and directories via the -X command for an alternate history file, which causes different error messages to be returned.

**•** CVE-2004-1428: FTP server generates an error message if the user name does not exist instead of prompting for a password, which allows remote attackers to determine valid usernames.

## Related Attack Patterns (CAPEC)

* CAPEC-331
* CAPEC-332
* CAPEC-541
* CAPEC-580

## Attack TTPs

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

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

## Modes of Introduction

**•** Architecture and Design: An observable response discrepancy frequently occurs during authentication, where a difference in failed-login messages could allow an attacker to determine if the username is valid or not. The discrepancy could be inadvertent (bug) or intentional (design).

**•** Implementation: An observable response discrepancy frequently occurs during authentication, where a difference in failed-login messages could allow an attacker to determine if the username is valid or not. The discrepancy could be inadvertent (bug) or intentional (design).

## Common Consequences

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

## Potential Mitigations

**•** 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)

**•** Implementation: Ensure that error messages only contain minimal details that are useful to the intended audience and no one else. The messages need to strike the balance between being too cryptic (which can confuse users) or being too detailed (which may reveal more than intended). The messages should not reveal the methods that were used to determine the error. Attackers can use detailed information to refine or optimize their original attack, thereby increasing their chances of success. If errors must be captured in some detail, record them in log messages, but consider what could occur if the log messages can be viewed by attackers. Highly sensitive information such as passwords should never be saved to log files. Avoid inconsistent messaging that might accidentally tip off an attacker about internal state, such as whether a user account exists or not. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** In the above code, there are different messages for when an incorrect username is supplied, versus when the username is correct but the password is wrong. This difference enables a potential attacker to understand the state of the login function, and could allow an attacker to discover a valid username by trying different values until the incorrect password message is returned. In essence, this makes it easier for an attacker to obtain half of the necessary authentication credentials.

## Notes

**•** Relationship: can overlap errors related to escalated privileges