# CWE Detail – CWE-841

## Description

The product supports a session in which more than one behavior must be performed by an actor, but it does not properly ensure that the actor performs the behaviors in the required sequence.

## Extended Description

By performing actions in an unexpected order, or by omitting steps, an attacker could manipulate the business logic of the product or cause it to enter an invalid state. In some cases, this can also expose resultant weaknesses. For example, a file-sharing protocol might require that an actor perform separate steps to provide a username, then a password, before being able to transfer files. If the file-sharing server accepts a password command followed by a transfer command, without any username being provided, the product might still perform the transfer. Note that this is different than CWE-696, which focuses on when the product performs actions in the wrong sequence; this entry is closely related, but it is focused on ensuring that the actor performs actions in the correct sequence. Workflow-related behaviors include: Steps are performed in the expected order. Required steps are not omitted. Steps are not interrupted. Steps are performed in a timely fashion.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2011-0348: Bypass of access/billing restrictions by sending traffic to an unrestricted destination before sending to a restricted destination.

**•** CVE-2007-3012: Attacker can access portions of a restricted page by canceling out of a dialog.

**•** CVE-2009-5056: Ticket-tracking system does not enforce a permission setting.

**•** CVE-2004-2164: Shopping cart does not close a database connection when user restores a previous order, leading to connection exhaustion.

**•** CVE-2003-0777: Chain: product does not properly handle dropped connections, leading to missing NULL terminator (CWE-170) and segmentation fault.

**•** CVE-2005-3327: Chain: Authentication bypass by skipping the first startup step as required by the protocol.

**•** CVE-2004-0829: Chain: File server crashes when sent a "find next" request without an initial "find first."

**•** CVE-2010-2620: FTP server allows remote attackers to bypass authentication by sending (1) LIST, (2) RETR, (3) STOR, or other commands without performing the required login steps first.

**•** CVE-2005-3296: FTP server allows remote attackers to list arbitrary directories as root by running the LIST command before logging in.

## Modes of Introduction

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

## Common Consequences

**•** Impact: Alter Execution Logic — Notes: An attacker could cause the product to skip critical steps or perform them in the wrong order, bypassing its intended business logic. This can sometimes have security implications.

## Demonstrative Examples

**•** The server correctly avoids sending files to a user that isn't logged in and doesn't own the file. However, the server will incorrectly list the files in any directory without confirming the command came from an authenticated user, and that the user is authorized to see the directory's contents.

## Notes

**•** Research Gap: This weakness is typically associated with business logic flaws, except when it produces resultant weaknesses. The classification of business logic flaws has been under-studied, although exploitation of business flaws frequently happens in real-world systems, and many applied vulnerability researchers investigate them. The greatest focus is in web applications. There is debate within the community about whether these problems represent particularly new concepts, or if they are variations of well-known principles. Many business logic flaws appear to be oriented toward business processes, application flows, and sequences of behaviors, which are not as well-represented in CWE as weaknesses related to input validation, memory management, etc.