# CWE Detail – CWE-768

## Description

The product contains a conditional statement with multiple logical expressions in which one of the non-leading expressions may produce side effects. This may lead to an unexpected state in the program after the execution of the conditional, because short-circuiting logic may prevent the side effects from occurring.

## Extended Description

Usage of short circuit evaluation, though well-defined in the C standard, may alter control flow in a way that introduces logic errors that are difficult to detect, possibly causing errors later during the product's execution. If an attacker can discover such an inconsistency, it may be exploitable to gain arbitrary control over a system. If the first condition of an "or" statement is assumed to be true under normal circumstances, or if the first condition of an "and" statement is assumed to be false, then any subsequent conditional may contain its own logic errors that are not detected during code review or testing. Finally, the usage of short circuit evaluation may decrease the maintainability of the code.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context — Notes: Widely varied consequences are possible if an attacker is aware of an unexpected state in the product after a conditional. It may lead to information exposure, a system crash, or even complete attacker control of the system.

## Potential Mitigations

**•** Implementation: Minimizing the number of statements in a conditional that produce side effects will help to prevent the likelihood of short circuit evaluation to alter control flow in an unexpected way. (Effectiveness: N/A)

## Demonstrative Examples

**•** When compiled and run, the above code will output a privilege level of 1, or PRIV\_REGULAR for every user but the user with id 0 since the prefix increment operator used in the if statement will reach zero and short circuit before setting the 0th user's privilege level. Since we used calloc, this privilege will be set to 0, or PRIV\_ADMIN.