Secrets
ABAP
Apex
C
C++
CloudFormation
COBOL
C#
CSS
Flex
Go
HTML
Java
JavaScript
Kotlin
Kubernetes
Objective C
PHP
PL/I
PL/SQL
Python
RPG
Ruby
Scala
Swift
Terraform
Text
TypeScript
T-SQL
VB.NET
VB6
XML

C++ static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your C++ code

All rules 578 | Vulnerability 13 | Bug 111 | Security Hotspot 18 | Code Smell 436 | Quick Fix 68

Tags

Search by name...

"memset" should not be used to delete sensitive data
Vulnerability

POSIX functions should not be called with arguments that trigger buffer overflows
Vulnerability

XML parsers should not be vulnerable to XXE attacks
Vulnerability

Function-like macros should not be invoked without all of their arguments
Bug

The address of an automatic object should not be assigned to another object that may persist after the first object has ceased to exist
Bug

Assigning to an optional should directly target the optional
Bug

Result of the standard remove algorithms should not be ignored
Bug

"std::scoped_lock" should be created with constructor arguments
Bug

Objects should not be sliced
Bug

Immediately dangling references should not be created
Bug

"pthread_mutex_t" should be unlocked in the reverse order they were locked
Bug

"pthread_mutex_t" should be properly

The right-hand operands of && and || should not contain side effects

Analyze your code

Code Smell | Blocker | based-on-misra cert

There are some situations in C++ where certain parts of expressions may not be evaluated. If these sub-expressions contain side effects then those side effects may or may not occur, depending on the values of other sub expressions. The operators which can lead to this problem are `&&` and `||`, where the evaluation of the right-hand operand is conditional on the value of the left-hand operand. The conditional evaluation of the right-hand operand of one of the logical operators can easily cause problems if the developer relies on a side effect occurring.

Operations that cause side effects are:

- accessing a volatile object
- modifying an object
- modifying a file
- calling a function that performs any operations that cause changes in the state of the execution environment of the calling function.

This rule raises an issue when there is assignment or the use of the increment/decrement operators in right-hand operands.

Noncompliant Code Example

```
if ( ishigh && ( x == i++ ) ) // Noncompliant
...
if ( ishigh && ( x ==  getX() ) ) // Only acceptable if getX(
```

The operations that cause side effects are accessing a volatile object, modifying an object, modifying a file, or calling a function

that does any of those operations, which cause changes in the state of the execution environment of the calling function.

For the time being, this rule only check that there is no assignment or no use of increment/decrement operators made in right hand operands.

See

- MISRA C:2004, 12.4 - The right-hand operand of a logical && or || operator shall not contain side effects.
- MISRA C++:2008, 5-14-1 - The right hand operand of a logical && or || operator shall not contain side effects.
- MISRA C:2012, 13.5 - The right hand operand of a logical && or || operator shall not contain persistent side effects
- CERT, EXP02-C. - Be aware of the short-circuit behavior of the logical AND and OR operators

Available In:

sonarlint | sonarcloud | sonarqube Developer Edition

initialized and destroyed

Bug

"pthread_mutex_t" should not be consecutively locked or unlocked twice

Bug

"std::move" and "std::forward" should not be confused

Bug

A call to "wait()" on a "std::condition_variable" should have a