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

Stack allocated memory and non-owned memory should not be freed

Bug | Blocker | symbolic-execution | unpredictable

Stack allocated memory, like memory allocated with the functions `alloca`, `_alloca`, `_malloca`, `__builtin_alloca`, is automatically released at the end of the function, and should not be released with `free`. Explicitly `free`-ing such memory results in undefined behavior.

This rule raises issues when trying to release pointers to memory which is not owned, like stack allocated memory and function pointers.

Noncompliant Code Example

```
void fun() {
  char *name = (char *) alloca(size);
  // ...
  free(name); // Noncompliant, memory allocated on the stack
  char *name2 = "name";
  // ...
  free(name2); // Noncompliant, memory allocated on the stack
}
```

Compliant Solution

```
void fun() {
  char *name = (char *) alloca(size);
  // ...
  char *name2 = "name";
  // ...
}
```

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