O Quick 68 Fix







All 578

rules

## C++ static code analysis

6 Vulnerability (13)

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

**R** Bug (111)

Security

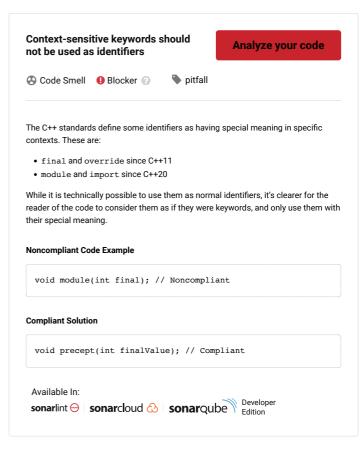
Hotspot

Tags

18

"memset" should not be used to delete sensitive data
POSIX functions should not be called with arguments that trigger buffer overflows
<b>읍</b> Vulnerability
XML parsers should not be vulnerable to XXE attacks
<b>읍</b> 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
<b>∰</b> Bug
Result of the standard remove algorithms should not be ignored
<b>R</b> Bug
"std::scoped_lock" should be created with constructor arguments
क्रै Bug
Objects should not be sliced
<b>♣</b> Bug
Immediately dangling references should not be created
<b>∰</b> Bug
"pthread_mutex_t" should be unlocked in the reverse order they were locked

"pthread\_mutex\_t" should be properly



© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective

owners. All rights are expressly reserved.
Privacy Policy

Smell 436

Search by name.

initialized and destroyed

in Bug

"pthread\_mutex\_t" should not be consecutively locked or unlocked twice

in Bug

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

in Bug

A call to "wait()" on a "std::condition\_variable" should have a