



C C

CloudFormation

COBOL COBOL

C# C#

CSS

⊠ Flex

-co Go

₩ HTML

🔮 Java

Js JavaScript

Kotlin

Kubernetes

Objective C

PHP

PL/I

PL/SQL

🦆 Python

RPG RPG

Ruby

Scala

Swift

Terraform

■ Text

Ts TypeScript

T-SQL

VB VB.NET

VB6 VB6

xmL XML



C static code analysis

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

All 311 rules

Wulnerability 13

Bug 74

Security 18

Hotspot

Code 206

Smell

Quick 14

Fix

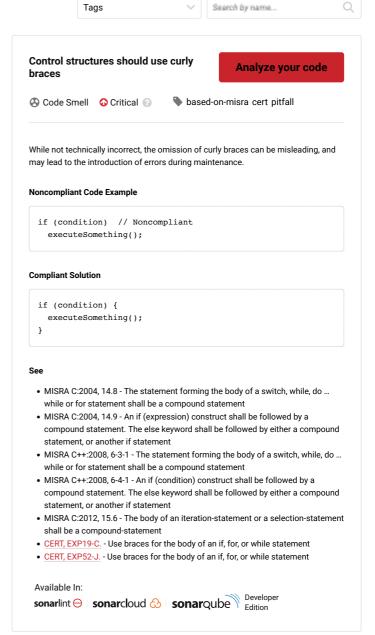
"memset" should not be used to delete sensitive data Vulnerability POSIX functions should not be called with arguments that trigger buffer overflows Vulnerability XML parsers should not be vulnerable to XXE attacks Vulnerability Function-like macros should not be invoked without all of their arguments ₩ 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 "pthread_mutex_t" should be unlocked in the reverse order they were locked "pthread_mutex_t" should be properly initialized and destroyed # Bua "pthread_mutex_t" should not be consecutively locked or unlocked # Bug Functions with "noreturn" attribute should not return # Bug

"memcmp" should only be called with

pointers to trivially copyable types

with no padding

🖷 Bug



© 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

Stack allocated memory and nonowned memory should not be freed

R
Bug

Closed resources should not be accessed

Bug

Dynamically allocated memory should be released

Bug

Freed memory should not be used