O Quick 14





XML



ΑII 311

rules

C static code analysis

6 Vulnerability (13)

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

n Bug 74

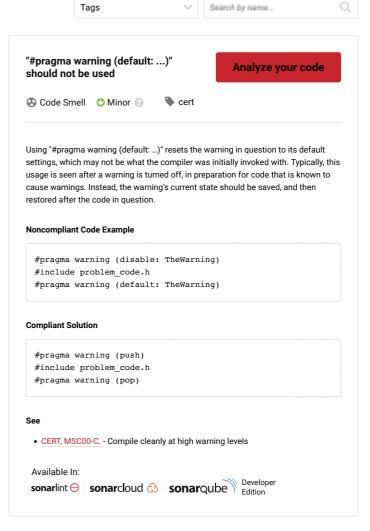
o Security

Hotspot

18

	•
"memset"	' should not be used to delete data
6 Vulner	rability
	nctions should not be called ments that trigger buffer
6 Vulner	rability
XML pars to XXE at	ers should not be vulnerable tacks
6 Vulner	rability
	like macros should not be vithout all of their arguments
🕀 Bug	
should no object tha	ess of an automatic object ot be assigned to another at may persist after the first s ceased to exist
	mutex_t" should be unlocked erse order they were locked
<table-of-contents> Bug</table-of-contents>	
•	mutex_t" should be properly I and destroyed
<table-of-contents> Bug</table-of-contents>	
	mutex_t" should not be ively locked or unlocked
👬 Bug	
Functions should no	s with "noreturn" attribute ot return
👬 Bug	
	p" should only be called with to trivially copyable types adding

👬 Bug



⊕ Code 206

Smell

© 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