O Quick 14







All 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

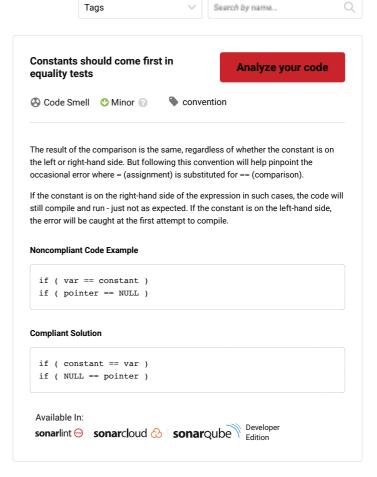
18

"memset" sensitive o	should not be used to delete data
6 Vulner	ability
	octions should not be called ments that trigger buffer
6 Vulner	ability
XML parse to XXE att	ers should not be vulnerable acks
6 Vulnera	ability
	ike macros should not be ithout all of their arguments
<table-of-contents> Bug</table-of-contents>	
should not object that	ess of an automatic object t be assigned to another t may persist after the first s ceased to exist
<table-of-contents> Bug</table-of-contents>	
	mutex_t" should be unlocked erse order they were locked
🕕 Bug	
	nutex_t" should be properly and destroyed
<table-of-contents> Bug</table-of-contents>	
	mutex_t" should not be vely locked or unlocked
<table-of-contents> Bug</table-of-contents>	
Functions should not	with "noreturn" attribute t return
<table-of-contents> Bug</table-of-contents>	
"momomn	" should only be called with

pointers to trivially copyable types

with no padding

👬 Bug



Smell 206

© 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