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

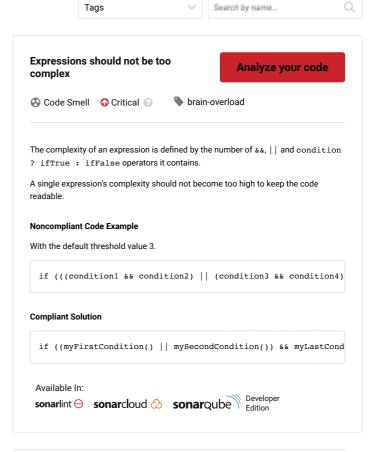
Hotspot

18

	emset" should not be used to delete sitive data
	Vulnerability
with	SIX functions should not be called h arguments that trigger buffer rflows
6	Vulnerability
	L parsers should not be vulnerable (XE attacks
6	Vulnerability
	action-like macros should not be oked without all of their arguments
Ŵ	Bug
sho obje	e address of an automatic object ould not be assigned to another ect that may persist after the first ect has ceased to exist
Ŵ	Bug
	nread_mutex_t" should be unlocked he reverse order they were locked
Ĥŧ	Bug
	nread_mutex_t" should be properly ialized and destroyed
Ĥŧ	Bug
	nread_mutex_t" should not be secutively locked or unlocked ce
Ĥŧ	Bug
	actions with "noreturn" attribute ould not return
	Bug

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