O Quick 14







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

₩ Bug (74)

Security

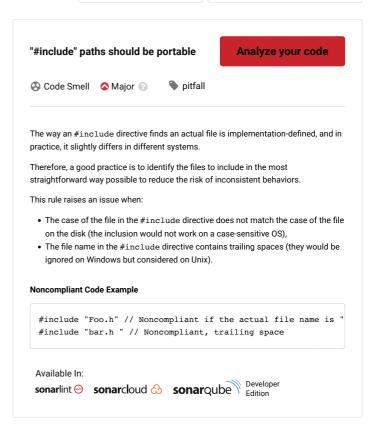
Hotspot

Tags

18

_	
	"memset" should not be used to delete sensitive data
	⑥ Vulnerability
	POSIX functions should not be called with arguments that trigger buffer overflows
	6 Vulnerability
	XML parsers should not be vulnerable to XXE attacks
	읍 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
	it Bug
	"pthread_mutex_t" should be unlocked in the reverse order they were locked
	👬 Bug
	"pthread_mutex_t" should be properly initialized and destroyed
	∰ Bug
	"pthread_mutex_t" should not be consecutively locked or unlocked twice
	👚 Bug
	Functions with "noreturn" attribute should not return
	∰ Bug
	"memcmp" should only be called with pointers to trivially copyable types with no padding

🖷 Bug



⊗ Code

Smell

206

Search by name.

© 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