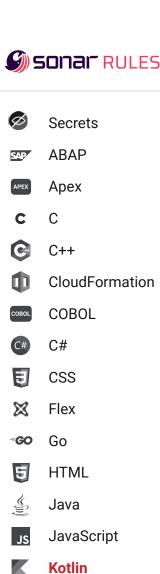
Code Smell (56)

Search by name...





Kubernetes

Objective C

PHP

PL/I

PL/SQL

Python

RPG

Ruby

Scala

Swift

Text

T-SQL

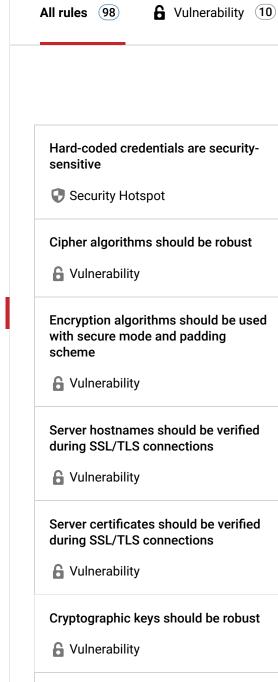
VB.NET

VB6

XML

Terraform

TypeScript



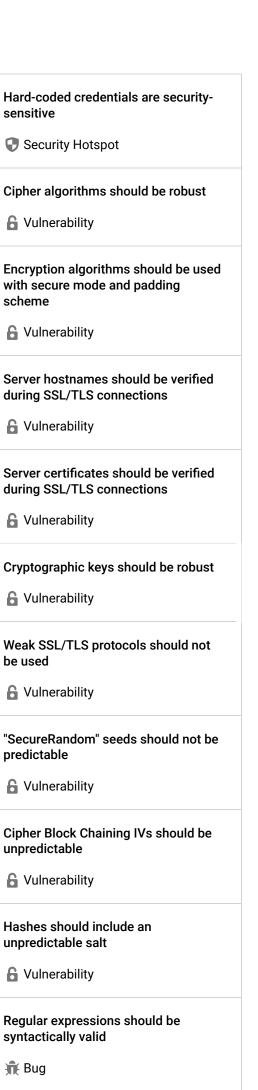
Kotlin static code analysis

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

R Bug (17)

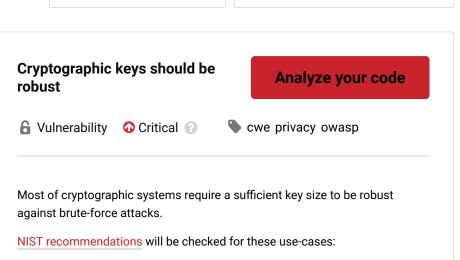
Tags

Security Hotspot (15)



"runFinalizersOnExit" should not be

🛊 Bug



Digital Signature Generation and Verification:

- p \geq 2048 AND q \geq 224 for DSA (p is key length and q the modulus length)
- $n \ge 2048$ for RSA (n is the key length)

Key Agreement:

- p ≥ 2048 AND q ≥ 224 for DH and MQV
- n ≥ 224 for ECDH and ECMQV (Examples: secp192r1 is a non-compliant curve (n < 224) but secp224k1 is compliant (n >= 224))

Symmetric keys:

• key length ≥ 128 bits

This rule will not raise issues for ciphers that are considered weak (no matter the key size) like DES, Blowfish.

Noncompliant Code Example

val keyPairGen1 = KeyPairGenerator.getInstance("RSA") keyPairGen1.initialize(1024) // Noncompliant val keyPairGen5 = KeyPairGenerator.getInstance("EC") val ecSpec1 = ECGenParameterSpec("secp112r1") // Noncomp keyPairGen5.initialize(ecSpec1) val keyGen1 = KeyGenerator.getInstance("AES") keyGen1.init(64) // Noncompliant

Compliant Solution

val keyPairGen6 = KeyPairGenerator.getInstance("RSA") keyPairGen6.initialize(2048) // Compliant val keyPairGen5 = KeyPairGenerator.getInstance("EC") val ecSpec1 = ECGenParameterSpec("secp256r1") // Complia keyPairGen5.initialize(ecSpec1) val keyGen2 = KeyGenerator.getInstance("AES") keyGen2.init(128) // Compliant

See

- OWASP Top 10 2021 Category A2 Cryptographic Failures
- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 Security Misconfiguration
- Mobile AppSec Verification Standard Cryptography Requirements
- OWASP Mobile Top 10 2016 Category M5 Insufficient Cryptography
- NIST 800-131A Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
- MITRE, CWE-326 Inadequate Encryption Strength

"ScheduledThreadPoolExecutor" should not have 0 core threads Rug Bug Jump statements should not occur in "finally" blocks Rug Bug Using clear-text protocols is securitysensitive Security Hotspot Accessing Android external storage is security-sensitive Security Hotspot Receiving intents is security-sensitive Security Hotspot Broadcasting intents is securitysensitive Security Hotspot Using weak hashing algorithms is security-sensitive Security Hotspot Using pseudorandom number generators (PRNGs) is securitysensitive Security Hotspot Empty lines should not be tested with regex MULTILINE flag Code Smell **Cognitive Complexity of functions**

should not be too high

Code Smell

Available In:
sonarlint ⊖ | sonarcloud ↔ | sonarqube

© 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