Security

Hotspot

Tags

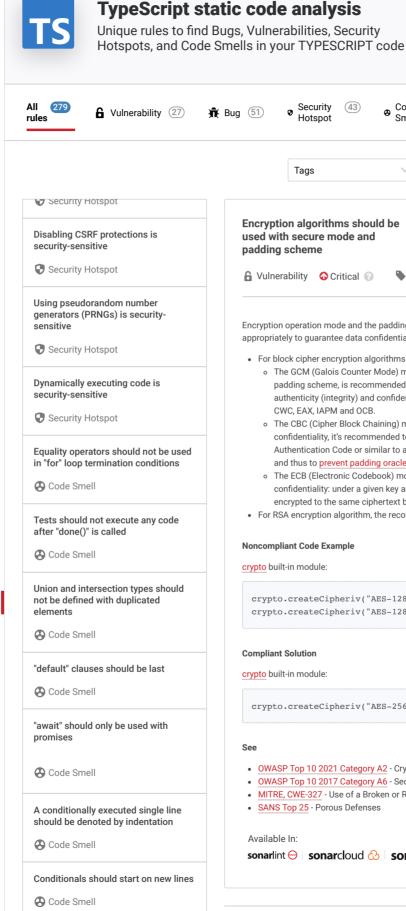
(43)



Products ✓

O Quick 50 Fix





Cognitive Complexity of functions

should not be too high

Code Smell

Encryption algorithms should be used with secure mode and Analyze your code padding scheme cwe privacy owasp sans-top25 Encryption operation mode and the padding scheme should be chosen appropriately to guarantee data confidentiality, integrity and authenticity: • For block cipher encryption algorithms (like AES): The GCM (Galois Counter Mode) mode which works internally with zero/no padding scheme, is recommended, as it is designed to provide both data authenticity (integrity) and confidentiality. Other similar modes are CCM, CWC, EAX, IAPM and OCB. o The CBC (Cipher Block Chaining) mode by itself provides only data confidentiality, it's recommended to use it along with Message Authentication Code or similar to achieve data authenticity (integrity) too and thus to prevent padding oracle attacks. The ECB (Electronic Codebook) mode doesn't provide serious message confidentiality: under a given key any given plaintext block always gets encrypted to the same ciphertext block. This mode should not be used. • For RSA encryption algorithm, the recommended padding scheme is OAEP. Noncompliant Code Example crypto built-in module crypto.createCipheriv("AES-128-CBC", key, iv); // Noncomplia crypto.createCipheriv("AES-128-ECB", key, ""); // Noncomplia **Compliant Solution** crypto built-in module: crypto.createCipheriv("AES-256-GCM", key, iv); OWASP Top 10 2021 Category A2 - Cryptographic Failures OWASP Top 10 2017 Category A6 - Security Misconfiguration MITRE, CWE-327 - Use of a Broken or Risky Cryptographic Algorithm SANS Top 25 - Porous Defenses Available In: sonarlint ⊕ | sonarcloud ♦ | sonarqube

⊗ Code

Smell

(158)

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

"void" should not be used

Code Smell

Loop counters should not be assigned to from within the loop body

Code Smell

"for" loop increment clauses should modify the loops' counters

Code Smell

Functions should not be empty

Code Smell