O Quick 68 Fix







ΑII 578

# C++ static code analysis

6 Vulnerability (13)

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

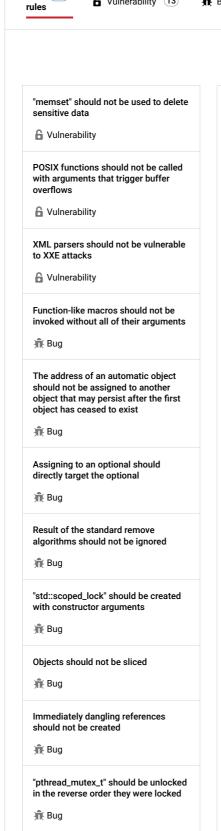
**R** Bug (111)

Security

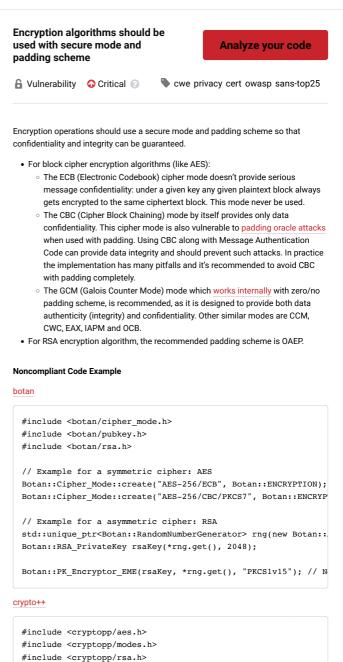
Hotspot

Tags

18



"pthread\_mutex\_t" should be properly



// Example for a symmetric cipher: AES

// Example for a asymmetric cipher: RSA

OpenSSL

CryptoPP::ECB Mode<CryptoPP::AES>::Encryption(); // Noncompli

CryptoPP::CBC\_Mode<CryptoPP::AES>::Encryption(); // Noncompli

CryptoPP::RSAES<CryptoPP::PKCS1v15>::Encryptor(); // Noncompl

⊗ Code

Smell

436

Search by name.

## initialized and destroyed

👬 Bug

"pthread\_mutex\_t" should not be consecutively locked or unlocked twice

# Bua

"std::move" and "std::forward" should not be confused

🖷 Bug

A call to "wait()" on a "std::condition\_variable" should have a

```
#include <openssl/evp.h>
#include <openssl/rsa.h>

// Example for a symmetric cipher: AES
EVP_aes_128_ecb(); // Noncompliant
EVP_aes_128_cbc(); // Noncompliant

// Example for a asymmetric cipher: RSA
RSA_public_decrypt(flen, from, to, key, RSA_PKCS1_PADDING); /
RSA_public_decrypt(flen, from, to, key, RSA_SSLV23_PADDING);
RSA_public_decrypt(flen, from, to, key, RSA_NO_PADDING); // N
```

### Compliant Solution

#### botan

```
#include <botan/cipher_mode.h>
#include <botan/pubkey.h>
#include <botan/rsa.h>

// AES symmetric cipher is recommended to be used with GCM mo
Botan::Cipher_Mode::create("AES-256/GCM", Botan::ENCRYPTION);

// RSA asymmetric cipher is recommended to be used with OAEP
std::unique_ptr<Botan::RandomNumberGenerator> rng(new Botan::Botan::RSA_PrivateKey rsaKey(*rng.get(), 2048);

Botan::PK_Encryptor_EME(rsaKey, *rng.get(), "OAEP"); // Compl
```

### crypto++

```
#include <cryptopp/gcm.h>
// AES symmetric cipher is recommended to be used with GCM mo
CryptoPP::GCM<CryptoPP::AES>::Encryption(); // Compliant
// RSA asymmetric cipher is recommended to be used with OAEP
CryptoPP::RSAES<CryptoPP::OAEP<CryptoPP::SHA1>>::Encrypto();
```

## OpenSSL

```
#include <openssl/evp.h>

// AES symmetric cipher is recommended to be used with GCM mo
EVP_aes_128_gcm() // Compliant

// RSA asymmetric cipher is recommended be used with OAEP pad
RSA_public_decrypt(flen, from, to, key, RSA_PKCS1_OAEP_PADDIN
```

## See

- 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 Developer Edition

© 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