FB.STATIC\_IV

Ошибка "The initialization vector (IV) is not properly generated" указывает на проблемы с созданием правильного вектора инициализации (IV) в криптографических операциях, чаще всего связанных с использованием алгоритмов симметричного шифрования, таких как AES (Advanced Encryption Standard).

В симметричном шифровании ключ используется как для шифрования, так и для дешифрования данных. Вместе с ключом часто используется вектор инициализации (IV), который добавляется к ключу перед шифрованием. Неправильная генерация IV может привести к уязвимостям в системе шифрования

Таблица №1 – Основные характеристики детектора FB.STATIC\_IV

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Static Initialization Vector |
| CWE | CWE329 |
| CVE | --- |
| Возможные последствия | Уязвимость шифрования, возможность взлома зашифрованных данных, нарушение конфиденциальности информации |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() throws Exception {  KeyGenerator keyGen = KeyGenerator.getInstance("AES");  SecretKey key = keyGen.generateKey();    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");  cipher.init(Cipher.ENCRYPT\_MODE, key, new IvParameterSpec(STATIC\_IV)); // Уязвимость!    byte[] encrypted = cipher.doFinal("Секретное сообщение".getBytes());  System.out.println("Небезопасное шифрование завершено");  } | public static void correctTest() throws Exception {  KeyGenerator keyGen = KeyGenerator.getInstance("AES");  SecretKey key = keyGen.generateKey();    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");    // Безопасно: генерация уникального IV для каждой операции  SecureRandom random = new SecureRandom();  byte[] iv = new byte[16];  random.nextBytes(iv);    cipher.init(Cipher.ENCRYPT\_MODE, key, new IvParameterSpec(iv));  byte[] encrypted = cipher.doFinal("Секретное сообщение".getBytes());  System.out.println("Безопасное шифрование завершено");  } |