FB.EI\_EXPOSE\_REP2

Этот код сохраняет ссылку на внешний изменяемый объект во внутреннем представлении объекта. Если доступ к экземплярам осуществляется с помощью ненадежного кода, а непроверенные изменения изменяемого объекта могут привести к нарушению безопасности или других важных свойств, нужно будет сделать что-то другое. Сохранение копии объекта является лучшим подходом во многих ситуациях.

Таблица №1 – Основные характеристики детектора FB.EI\_EXPOSE\_REP2

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Exposure of Internal Representation |
| CWE | CWE374 |
| CVE | --- |
| Возможные последствия | Нарушение инкапсуляции; непредсказуемые изменения состояния объекта извне; потенциальные уязвимости, если объект используется в критических операциях |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  SecureDataHolder holder = new SecureDataHolder(new int[]{1, 2, 3});  int[] data = holder.getData(); // ОШИБКА: возврат ссылки на внутренний массив  data[0] = 999; // Изменение внутреннего состояния объекта  System.out.println("Modified data (INCORRECT): " + Arrays.toString(holder.getData()));  } | public static void correctTest() {  SecureDataHolderFixed holder = new SecureDataHolderFixed(new int[]{1, 2, 3});  int[] data = holder.getData(); // Возвращает копию массива  data[0] = 999; // Не влияет на внутренний массив  System.out.println("Original data preserved (CORRECT): " + Arrays.toString(holder.getData()));  } |