FB.EI\_EXPOSE\_STATIC\_REP2

Этот код сохраняет ссылку на внешне изменяемый объект в статическом поле. Если непроверенные изменения изменяемого объекта поставят под угрозу безопасность или другие важные свойства, следует это исправить. Во многих ситуациях лучше хранить копию объекта.

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

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Exposed Static Mutable Field |
| CWE | CWE-218 |
| CVE | --- |
| Возможные последствия | Несанкционированная модификация критических данных; нарушение инкапсуляции и принципов ООП; гонки данных в многопоточной среде; неожиданное поведение системы из-за внешнего изменения состояния |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  // Модификация извне  UNSAFE\_KEYS.add("hacked\_key");  ADMIN\_NAMES[0] = "attacker";  } | public static void correctTest() {  // Безопасный доступ через методы  addKey("secure\_key");  getAdminNames()[0] = "try\_hack"; // Не изменит реальный массив  } |

Методы устранения уязвимости при срабатывании детектора.

1. Инкапсуляция полей;
2. Защитное копирование для массивов;
3. Неизменяемые представления коллекций;
4. Thread-safe обертки.