FB.MS\_CANNOT\_BE\_FINAL

Изменяемое статическое поле может быть изменено вредоносным кодом или случайно из другого пакета. К сожалению, способ использования поля не позволяет легко решить эту проблему.

Таблица №1 – Основные характеристики детектора FB.MS\_CANNOT\_BE\_FINAL

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Mutable Static Field Without Final |
| CWE | CWE-218 |
| CVE | --- |
| Возможные последствия | Несанкционированная модификация данных, доступных глобально; непредсказуемое поведение системы из-за изменений статического состояния; гонки данных в многопоточной среде; нарушение инкапсуляции и принципов ООП. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  // Изменение ссылки на статическое поле  UNSAFE\_LIST = new ArrayList<>(); // Опасная операция!    // Модификация содержимого  INTERNAL\_DATA[0] = "Hacked";  } | public static void correctTest() {  // Безопасное использование через методы  addToSafeList("Value");  String[] copy = getReadonlyData(); // Защитная копия  copy[0] = "Try"; // Не влияет на оригинал  } |

Методы устранения уязвимости при срабатывании детектора.

1. Объявите статические поля как final;
2. Используйте защитное копирование;
3. Неизменяемые коллекции;
4. Синхронизация для потокобезопасности;
5. Статические фабричные методы.