FB.MS\_SHOULD\_BE\_FINAL

Это общедоступное статическое или защищенное статическое поле не является окончательным и может быть изменено вредоносным кодом или случайно из другого пакета. Чтобы избежать этой уязвимости, поле лучше сделать окончательным.

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

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Security Vulnerability (Mutable Static Field) |
| CWE | CWE218 |
| CVE | --- |
| Возможные последствия | Непреднамеренное изменение статического поля из разных частей программы, приводящее к неожиданным побочным эффектам; возможность атак, если поле содержит критически важные данные (например, конфигурацию или временные токены). |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  // Вредоносный код или ошибка может перезаписать значение  ConfigIncorrect.API\_KEY = "hacked\_key";  System.out.println("Incorrect API Key: " + ConfigIncorrect.API\_KEY); // "hacked\_key"  } | public static void correctTest() {  // Попытка изменения final-поля приведёт к ошибке компиляции  // ConfigCorrect.API\_KEY = "new\_key"; // Ошибка: cannot assign a value to final variable  System.out.println("Correct API Key: " + ConfigCorrect.API\_KEY); // "secure\_key"  } |