FB.MS\_MUTABLE\_ARRAY

Последнее статическое поле ссылается на массив, к которому можно получить доступ с помощью вредоносного кода или случайно, через другой пакет. Этот код может свободно изменять содержимое массива.

Таблица №1 – Основные характеристики детектора FB.MS\_MUTABLE\_ARRAY

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | Unknown |
| Источник | SpotBugs |
| Тип ошибки | Data Encapsulation Vulnerability |
| CWE | CWE-218 |
| CVE | --- |
| Возможные последствия | Несанкционированная модификация данных: внешний код может изменять содержимое массива без ведома класса-владельца; нарушение целостности состояния: непредсказуемое поведение приложения из-за несогласованных изменений массива; утечка информации. |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest() {  Configuration.configParams[0] = "modified\_value"; // Прямая модификация массива  System.out.println("Некорректное значение: " + Configuration.configParams[0]);  } | public static void correctTest() {  ImmutableConfig.updateParameter(0, "secure\_value");  System.out.println("Защищенное значение: " + ImmutableConfig.getParameter(0));  } |